|  |  |
| --- | --- |
| 3GPP TR 33.861 V1.6.0 (2020-05) | |
|  | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on evolution of Cellular IoT security for the 5G System;  (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 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.  © 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 |

Contents

Introduction 9

2 References 10

3 Definitions of terms, symbols and abbreviations 11

3.1 Terms 11

3.2 Symbols 11

3.3 Abbreviations 11

4 Security aspects of the CIoT features in the 5G System 12

4.1 Background 12

4.2 High level potential security requirements 12

5 Key issues 12

5.1 Key Issue #1: Efficient frequent small data transmissions 12

5.1.1 Key issue details 12

5.1.2 Security threats 12

5.1.3 Potential security requirements 12

5.2 Key Issue #2: Integrity protection of small data 12

5.2.1 Key issue details 12

5.2.2 Security threats 13

5.2.3 Potential security requirements 13

5.3 Key Issue #3: Encryption of small data 13

5.3.1 Key issue details 13

5.3.2 Security threats 13

5.3.3 Potential security requirements 14

5.4 Key Issue #4: Signalling overload due to Malicious Applications on the UE 14

5.4.1 Introduction 14

5.4.2 Security Threats 14

5.4.3 Potential security requirements 14

5.5 Key Issue #5: gNB Protection from CIoT DoS attack 14

5.5.1 Key issue details 14

5.5.2 Security threats 15

5.5.3 Potential Security requirements 15

5.6 Key issue #6: Avoiding AS security for application security enabled UEs. 15

5.6.1 Potential security threat 15

5.6.2 Potential security requirements 15

5.7 Key Issue #7: Key refreshing for protection of small data 15

5.7.1 Key issue details 15

5.7.2 Security threats 16

5.7.3 Potential security requirements 16

5.8 Key Issue #8: Key and mac size for protection of small data 16

5.8.1 Key issue details 16

5.8.2 Security threats 16

5.8.3 Potential security requirements 16

5.9 Key Issue #9: Protection of NIDD interfaces 16

5.9.2 Security Threats 17

5.9.3 Potential security requirements 17

5.10 Key issue #10: User Plane data transmission with Connectionless signalling. 17

5.10.1 Description 17

5.10.2 Potential security threat 17

5.10.3 Potential security requirements 17

5.11 Key Issue #11: Bidding down attack for NAS based redirection between core networks 18

5.11.1 Key issue details 18

5.11.2 Security threats 18

5.11.3 Potential security requirements 18

5.12 Key Issue #12: Privacy protection of new parameters for CIoT included in NAS message 18

5.12.1 Key issue details 18

5.12.2 Security threats 19

5.12.3 Potential security requirements 19

5.13 Key Issue #13: Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC 19

5.13.1 Key issue details 19

5.13.2 Security threats 19

5.13.3 Potential security requirements 19

5.14 Key issue #14: Preventing User Plane Botnet Attacks from Improper CIOT Device Usage 20

5.14.1 Description 20

5.14.2 Potential security threat 20

5.14.3 Potential security requirements 20

5.15 Key Issue #15: Protection of UE capability transfer for UEs without AS security 20

5.15.1 Key issue details 20

5.15.2 Security threats 21

5.15.2 Potential security requirements 21

5.X Key Issue #X: <Key Issue Name> 21

5.X.1 Key issue details 21

5.X.2 Security threats 21

5.X.3 Potential security requirements 21

6 Solutions 21

6.1 Solution #1: Security Solution for small data transmission via NAS signaling 22

6.1.1 Introduction 22

6.1.2 Solution details 22

6.1.3 Evaluation 22

6.2 Solution #2: Efficient integrity protection for frequent small data transmissions 22

6.2.1 Introduction 22

6.2.2 Solution details 23

6.2.3 Evaluation 24

6.3 Solution #3: Security solution for MO SMS at AMF re-allocation 24

6.3.1 Introduction 24

6.3.2 Solution details 24

6.3.2.1 MO SMS included in initial NAS message 24

6.3.3 Evaluation 26

6.4 Solution #4: Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT) 26

6.4.1 Introduction 26

6.4.2 Solution details 27

6.4.2.1 UL data transmission from CM-IDLE (SUSPEND) with Early Data Transmission to old eNB 27

6.4.2.2 UL UP EDT from RRC SUSPEND to new eNB 28

6.4.2.3 Connection Suspend procedure using the Early Data Transmission (EDT) feature 28

6.4.3 Evaluation 28

6.5 Solution #5: Security solution for small data included in initial NAS signalling at mobility 29

6.5.1 Introduction 29

6.5.2 Solution details 29

6.5.3 Evaluation 31

6.6 Solution #6: Detecting and handling signalling overload due to Malicious Applications on the UE 31

6.6.1 Introduction 31

6.6.2 Solution details 32

6.6.2.1 Architecture 32

6.6.2.2 Procedures 33

6.6.3 Evaluation 34

6.7 Solution #7: Procedure for protecting gNB from RRC resume and RRC Re-establishment DoS attack 34

6.7.1 Introduction 34

6.7.2 Solution details 35

6.7.3 Evaluation 37

6.8 Solution #8: Security solution for protection of interface used by NIDD procedures 37

6.8.1 Introduction 37

6.8.2 Solution details 37

6.8.3 Evaluation 37

6.9 Solution #9: Security protection of small data at idle mobility 38

6.9.1 Introduction 38

6.9.2 Solution details 38

6.9.3 Evaluation 39

6.10 Solution #10: Security solution for small data at idle mobility using the Registration Complete message 39

6.10.1 Introduction 39

6.10.2 Solution details 39

6.10.3 Evaluation 40

6.11 Solution #11: Security-Property-Group-based Mitigation for DDoS Attack Triggered by Malicious Applications on the UE 40

6.11.1 Introduction 40

6.11.2 Solution details 41

6.11.2.1 Security-Property-Group assignment mechanism 41

6.11.2.1.1 Principle of assignment 41

6.11.2.1.2 Assignment Procedure 42

6.11.2.2 DDoS attack mitigation 42

6.11.2.2.1 DDoS attack on AMF/SMF 42

6.11.2.2.2 DDoS attack on UPF/NEF 42

6.11.3 Evaluation 43

6.12 Solution #12: Security Solution on DDoS attack mitigation 43

6.12.1 Introduction 43

6.12.2 Solution details 43

6.12.2.1 Architecture 43

6.12.2.2 Procedure 43

6.12.3 Evaluation 44

6.13 Solution #13: Security solution for small data using key refreshing 45

6.13.1 Introduction 45

6.13.2 Solution details 45

6.13.2.1 Support for infrequent small data transmission 45

6.13.2.2 Frequent small data communication 45

6.13.3 Evaluation 45

6.14 Solution #14: Privacy protection of new parameters for CIoT included in NAS messages 45

6.14.1 Introduction 45

6.14.2 Solution details 45

6.14.3 Evaluation 46

6.15 Solution #15: Efficient integrity protection for small data transmissions with immediate result 46

6.15.1 Introduction 46

6.15.2 Solution details 46

6.15.2.1 General 46

6.15.2.3 Receiver behaviour 47

6.15.3 Evaluation 47

6.16 Solution #16: Solution to Identify Misbehaving UEs 48

6.16.1 Introduction 48

6.16.2 Solution details 48

6.16.3 Evaluation 48

6.17 Solution #17: Solution to Mitigate DDoS Attack based on RAN caused by Massive Number of Misbehaving CIoT UEs 48

6.17.1 Introduction 48

6.17.2 Solution details 49

6.17.2.1 Architecture 49

6.17.2.2 Procedure 49

6.17.3 Evaluation 50

6.18 Solution #18: Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT) 51

6.18.1 Introduction 51

6.18.2 Solution details 51

6.18.2.1 UL data transmission from CM-IDLE with Early Data Transmission 51

6.18.2.2 Connection Suspend procedure using the Early Data Transmission (EDT) feature 52

6.18.3 Evaluation 52

6.19 Solution #19: Solution to Mitigate DDoS Attack on AMF caused by Massive Number of Misbehaving CIoT UEs 52

6.19.1 Introduction 52

6.19.2 Solution details 53

6.19.2.1 Architecture 53

6.19.2.2 Procedure 53

6.19.3 Evaluation 54

6.20 Solution 20: RRC Connection Re-Establishment for the Control Plane for NB-IoT connected to 5GC 55

6.20.1 Introduction 55

6.20.2 Solution Details 55

6.20.2.1 RRC Connection Re-Establishment Procedure without KAMF Change 55

6.20.2.2 RRC Connection Re-Establishment Procedure with KAMF Change 55

6.20.3 Evaluation 56

6.21 Solution 21: Protection of NAS Redirection Message 56

6.21.1 Introduction 56

6.21.2 Solution Details 57

6.21.2.1 Procedure of Authorization for Public Key of the AMF 57

6.21.2.2 Procedure of Protection of NAS message 58

6.21.2.3 Abnormal Cases 58

6.21.3 Evaluation 59

6.22 Solution #22: Security solution for UP IP in PDCP to protect UL EDT data in Msg 3 60

6.22.1 Introduction 60

6.22.2 Solution details 60

6.22.2.1 UL data transmission from CM-IDLE with Early Data Transmission 60

6.22.2.2 Connection Suspend procedure using the Early Data Transmission (EDT) feature 61

6.22.3 Evaluation 61

6.23 Solution #23: Mitigate DDoS Attack on RAN based on RANs coordination 62

6.23.1 Introduction 62

6.23.2 Solution details 62

6.23.3 Evaluation 62

6.24 Solution #24: Using NAS security for protection of NAS Redirection message 62

6.24.1 Introduction 62

6.24.2 Solution details 62

6.24.3 Evaluation 62

6.25 Solution #25: Security solution for preventing Botnet Attacks from Improper CIOT Device Use 63

6.25.1 Introduction 63

6.25.2 Solution A details 63

6.25.2 Solution B details 63

6.25.2 Solution C details 64

6.25.3 Evaluation 64

6.26 Solution #26: Hash based UE capability protection for CP optimization only CIoT UE 64

6.26.1 Introduction 64

6.26.2 Solution details 64

6.26.3 Evaluation 65

6.27 Solution #27: Network resilience for UEs without AS security 66

6.27.1 Introduction 66

6.27.2 Solution details 66

6.27.3 Evaluation 66

6.28 Solution #28: Protection of UE capability transfer for UEs without AS security 66

6.28.1 Introduction 66

6.28.2 Solution details 66

6.28.3 Evaluation 67

6.29 Solution #29: Security solution for UE Capability Transfer for UE with no AS security. 67

6.29.1 Introduction 67

6.29.2 Solution details 68

6.29.3 Evaluation 68

6.30 Solution #30: AMF verification of the UE radio capabilities for CP optimization only CIoT UE 68

6.30.1 Introduction 68

6.30.2 Solution details 69

6.30.3 Evaluation 70

6.Y Solution #Y: <Solution Name> 70

6.Y.1 Introduction 70

6.Y.2 Solution details 70

6.Y.3 Evaluation 70

7 Conclusions 70

7.1 Key Issue #1: Efficient frequent small data transmissions 70

7.2 Key Issue 2: Integrity protection of small data 70

7.3 Key Issue 3: Encryption of small data 70

7.4 Key Issue 4: Signalling overload due to Malicious Applications on the UE 70

7.5 Key Issue 5: gNB Protection from CIoT DoS attack 71

7.6 Key Issue 6: Avoiding AS security for application security enabled UEs. 71

7.7 Key Issue 7: Key refreshing for protection of small data 71

7.8 Key Issue 8: Key and mac size for protection of small data 71

7.9 Key Issue 9: Protection of NIDD interfaces 71

7.10 Key Issue 10: User Plane data transmission with Connectionless signalling. 71

7.11 Key Issue 11: Bidding down attack for NAS based redirection between core networks 71

7.12 Key Issue 12: Privacy protection of new parameters for CIoT included in NAS message 71

7.13 Key Issue 13: Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC 71

7.14 Key Issue 14: Preventing User Plane Botnet Attacks from Improper CIOT Device Usage 71

Annex A: Change history 73

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

The architectural study captured in 3GPP TR 23.724 [2] considers alternatives for supporting WB-EUTRA (eMTC) and/or NB-IoT in 5GS. The main assumption of the architectural study is that no new RAT for 5G massive MTC would be introduced but rather that the existing E-UTRAN radio technologies would be also used with 5GS. The 5GS already supports certain features that are useful for IoT, e.g. the UE can register to the system without necessarily establishing a PDU session and can use non-IP-type PDU sessions for data delivery. However, EPS provides also other features that are useful for IoT/MTC., e.g. power saving functions, overload control, high latency communication, monitoring, service capability exposure, etc. The extension of these EPS features to 5GS system is the main goal of the architectural study. Several of these features have security aspects. 1 Scope

The present document studies the following:

* Capture massive MTC related 5G requirements in other 3GPP documents and further analyse them from security point of view.
* Study security for supporting EPS CIoT/MTC functionalities in 5GS, e.g.
  + security for infrequent and frequent small data transmission
  + security for inter-RAT mobility to/from NB-IoT or modifications in the EPC-5GC interworking security specific to CIoT.
* Study security enhancements based on the architectural study in TR 23.724 [2], e.g.
  + security for transport of user plane over 5G NAS or
  + termination of user plane security in 5GC.
* Study the security aspects of the architectural enhancements addressing the 5G service requirements in TS 22.261 [3] and TR 38.913 [4].
* Study the need for additional mechanisms to improve protection of the network from maliciously behaving IoT devices

# 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 23.724: "Study on Cellular IoT support and evolution for the 5G System".

[3] 3GPP TS 22.261:"Service requirements for next generation new services and markets".

[4] 3GPP TR 38.913: "Study on scenarios and requirements for next generation access technologies".

[5] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 16)".

[6] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications (Release 16)".

[7] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 15)".

[9] 3GPP TR 23.724: "Study on Cellular IoT support and evolution for the 5G System (Release 15)".

[10] 3GPP TS 23.501: " System Architecture for the 5G System ".

[11] 3GPP TR 23.791: " Study of Enablers for Network Automation for 5G ".

[12] 3GPP TS 23.288: " Architecture enhancements for 5G System (5GS) to support network data analytics services. (Release 16) ".

[13] 3GPP TS 38.331 v15.4.0: " NR; Radio Resource Control (RRC) protocol specification (Release 15) ".

[14] 3GPP TS 38.300: " NR and NG-RAN Overall Description".

[15] 3GPP TS 23.502: " Procedures for the 5G System (Release 15) ".

[16] 3GPP TS 23.002: "Network architecture (Release 15)".

[17] S3-191848 "Handling of UE radio network capabilities in 4G and 5G".

[18] New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. https://doi.org/10.1145/3317549.3319728

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 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].

**example:** text used to clarify abstract rules by applying them literally.

**Misbehaving UE:** A UE that is controlled by an attacker with malicious application running.

**ng-eNB**: see definition in TS 38.300 [14].

**Narrowband-IoT (**NB-IoT**):** see definition in TS 23.401 [5]

## 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].

<ABBREVIATION> <Expansion>

5G-AN 5G Access Network

5G-RAN 5G Radio Access Network

AMF Access and Mobility Management Function

CIoT Cellular Internet of Things

CP Control Plane

DoS Denial of Service

DDoS Distributed Denial of Service

gNB NR Node B

IoT Internet of Things

MTC Machine Type of Communications

NB-IoT Narrow Band Internet of Things

NG Next Generation

ng-eNB Next Generation Evolved Node-B

NR New Radio

UPF User Plane Function

# 4 Security aspects of the CIoT features in the 5G System

## 4.1 Background

The architectural study in TR 23.724 [2] addresses two new 5G features related to service delivery for CIoT capable UEs. The first feature is for the infrequent transmission of small data. It is targeted at constrained, low power and low rate UEs. The solution for this feature makes use of the NAS signalling to transport the data similarly to the Data over NAS (DoNAS) feature in EPS. The second feature is for the frequent transmission of small data and is targeted at more active UEs. It is expected that the final solution for this feature will be based on a mixture of an enhanced version of RRC inactive with early data and the EPS resume suspend feature for Narrow Band IoT (NB-IoT). Since both features are based on the EPS ones, it is natural to expect similar security impact on the 5GS to support them.

## 4.2 High level potential security requirements

The security aspects shall be based on the CIoT architecture referring to TR 23.724 [2] where E-UTRAN (i.e. both WB-E-UTRA and NB-IoT) is connected to 5GC via N2/N3.

UEs used for CIoT in 5GS shall comply with the security features and security requirements in TS 33.501[8].

# 5 Key issues

## 5.1 Key Issue #1: Efficient frequent small data transmissions

### 5.1.1 Key issue details

There is a need to provide security solutions to support efficient frequent small data transmissions for low complexity, and low data-rate CIoT UEs. It is expected that the number of CIoT devices will increase exponentially leading to their massive deployment while the per device data amount whether transmitted or received will remain small.

### 5.1.2 Security threats

The security overhead for frequent data transmission from massively deployed low data-rate CIoT UEs may lead to DOS/DDOS on the availability of network services.

Lower than EPS security protection for frequent data transmission from a large number of CIoT UEs can serve as a vulnerability for exploits and network availability attacks on CIoT (e.g., bidding down attacks).

### 5.1.3 Potential security requirements

The system should limit the security overhead for frequent small data transmission.

The system security mechanisms shall ensure availability of the network and at least an equivalent level of security mechanisms, as in EPS, for a massive number of CIoT UEs with frequent small data transmission.

## 5.2 Key Issue #2: Integrity protection of small data

### 5.2.1 Key issue details

This key issue addresses the security aspects of key issue #1 and key issue #2 in SA2 TR 23.724 [2].

The 5G systems are expected to provide connectivity and other types of services to a massive number of devices simultaneously. Such devices include IoT devices that may send or receive infrequent or frequent small amounts of data. SA2 is studying several solutions for sending/receiving infrequent or frequent small data in their TR 23.724 [2].

Even if protection of small data is provided at application layer, there is still some value to add protection in the lower layers as it would protect the core network from malicious packets.

In 5G Rel-15, the UE and the AMF are mandatory to support integrity protection of NAS signalling in NAS layer. Integrity protection of NAS signalling is mandatory to use. The UE and the gNB are mandatory to support integrity protection of RRC signalling and user plane data in PDCP layer. Integrity protection of RRC signalling is mandatory to use. Integrity protection of user plane data is optional to use. The support of integrity protection of user plane data in PDCP layer was introduced as a new feature in Rel-15 compared to LTE. Not all UEs may support full data rate for integrity protection for DRBs in PDCP layer between UE and gNB. For example, if the UE indicates 64 kbps as its maximum data rate, then the network is assumed to turn on the integrity protection for user plane data only for data rates equal or lower than 64 kbps. Note that enhanced LTE eNB’s (i.e. ng-eNB) connected to a 5GC does not support integrity protection of user plane data in PDCP layer in Rel-15.

### 5.2.2 Security threats

If the infrequent or frequent small data is not integrity protected between the UE and network, then an attacker could modify the small data or even inject fake small data packets on behalf of the IoT device or the network on the air interface.

If integrity protection of small data is not provided by the lower layers, then any modification of the small data or any replayed small data can’t be detected by the lower layers, in order to avoid the delivery of the small data to the application layer for further processing.

### 5.2.3 Potential security requirements

The system shall support integrity protection and replay protection of small data.

The small data should be integrity and replay protected.

## 5.3 Key Issue #3: Encryption of small data

### 5.3.1 Key issue details

This key issue addresses key issue #1 and key issue #2 in SA2 TR 23.724 [2].

The 5G systems are expected to provide connectivity and other types of services to a massive number of devices simultaneously. Such devices include IoT devices that may send or receive infrequent or frequent small amount of data. SA2 is studying several solutions for sending/receiving infrequent or frequent small data in their TR 23.724 [2].

The small data sent over the air-interface is vulnerable to eavesdropping. Even if protection from eavesdropping of small data is provided at application layer, there is still some value to add protection from eavesdropping in the lower layers as it would protect against for example eavesdropping of headers as e.g. IP-headers etc.

In 5G Rel-15, the UE and the AMF are mandatory to support encryption of NAS signalling in NAS layer. Encryption of NAS signalling is optional to use in NAS layer. The UE and the gNB/ng-eNB are mandatory to support encryption of RRC signalling and user plane data in PDCP layer. Encryption of RRC signalling and user plane data is optional to use in PDCP layer. Encryption is activated independently for RRC signalling between UE and gNB/ng-eNB and for user plane data (per DRB) between UE and gNB/ng-eNB. Encryption is activated independently on NAS layer between UE and AMF and on PDCP layer between UE and gNB/ng-eNB.

### 5.3.2 Security threats

If the infrequent or frequent small data is not encrypted, an attacker could eavesdrop on the small data sent on the air interface.

### 5.3.3 Potential security requirements

The system shall support encryption of small data.

The small data may be confidentiality protected.

## 5.4 Key Issue #4: Signalling overload due to Malicious Applications on the UE

### 5.4.1 Introduction

A large number of UEs performing similar actions at the same time can easily lead to a signalling attack on the network. If such an attack persists and isn’t dealt with appropriately it brings a risk for other users of the network. As such, mitigating measures should be designed to protect the networks against such attacks.

For this key issue, it is assumed that the malicious behaviour on the UE is the result of an attacker having access to the application on the UE which it can instruct to make certain requests to the network. An attacker could have obtained this access through the over the top service and could for example instruct the UE to set up dedicated bearers or request access to certain network slices. Such procedures could lead to exhaustion of resources in both the radio and the core network, which would lead to denial of service or service degradation for other users of the network.

An important assumption of this key issue is that the UE part that is responsible for executing the radio instructions remains untouched. Also, it is assumed that the USIM is not compromised.

### 5.4.2 Security Threats

Denial of service due to signalling overload.

DDoS attacks towards the 5G core network include both large number of signal packets (e.g. NAS signalling messages) and user plane packets sent by compromised CIoT devices overloading the network. This kind of attack would lead to denial of service or at least throughput degradation caused by congestion to legitimate UEs whose traffic shares the same core network links. For example, access to the crucial core network functions (e.g. AMF) could be denied to normal UEs by one or more compromised UE(s) repeatedly initiate(s) authentication procedures in a short period.

### 5.4.3 Potential security requirements

1) The 5GS shall be able to identify UEs that are operating normally and UEs that are misbehaving.

2) The 5GS shall support a secure mechanism to isolate the misbehaving UEs from the network.

3) The 5G network shall be able to protect itself against signalling overload from specific (e.g. malicious) UEs.

## 5.5 Key Issue #5: gNB Protection from CIoT DoS attack

### 5.5.1 Key issue details

With the rapid growth of CIoT, there will be a massive number IoT devices connected to 5G network. IoT ecosystem is concerned that there is considerable high risk of large-scale service interruption due to possible CIoT DoS attacks. In addition, many IoT device developers are primarily concerned with CIoT devices internet functions rather than security. Not only that but some IoT device manufactures don’t even have secure production environment. These factors may introduce a large number of IoT devices with very weak security capabilities. Furthermore, most of IoT devices will be deployed in unmanned places where attackers can easily access and utilized these IoT devices to launch DoS attacks against the network.

gNB is the first gate for CIoT devices in 3GPP network; it faces serious threat of DoS attacks and it should provide solid security mechanism to identify and prevent DoS attacks from CIoT devices.

### 5.5.2 Security threats

In IoT scenarios, many IoT devices will be deployed densely such as smart meters and shared bicycles. Attackers can hijack these IoT devices which deployed approximately in same location to launch DoS attack on the control/user plane against the gNB by sending a large number of bogus packets to gNB. This attack could exhaust gNB resources, thus it cannot provide its fundamental function of internet access.

Maliciously the RRC signalling exchanged before AS security activation can be used to cause DoS attack to gNB. For example, attackers may compromise a large number of IoT devices to send access request messages repeatedly, send mass number of Random Access to gNB in a short time to occupy preamble to cause other normal IoT devices fail to access. Attack may also construct malicious RRC signalling to attack gNB.

After As security activation, IoT devices can be used maliciously to send a large number of signalling or user plane packets to gNB, for example, send massive RRC signalling or UP data such as, RRC re-establishment/RRC resume/User plane packets etc. to cause gNB exhaust the process resource to make the gNB deny service.

### 5.5.3 Potential Security requirements

1. gNB should support a mechanism to identify and mitigate DoS attack caused by RRC message.

## 5.6 Key issue #6: Avoiding AS security for application security enabled UEs.

Many CIoT devices are constrained devices communicating short packets of data for a very short duration. Such devices may lack dedicated resources for radio level encryption. In many such devices, end to end application layer encryption may be enabled between the application in the UE and the application server in the network. For such devices it may be sufficient to have only one level of encryption and hence can avoid the radio level encryption between the CIoT UE and the gNB.

Though radio level encryption is avoided, some CIoT UEs may need integrity protection to avoid any packet manipulation. But for some sensor devices even this radio level integrity protection also may be not needed because of the very small amount of data. Hence the gNB need to support all combinations of integrity and encryption activation and deactivation for CIoT UEs.

### 5.6.1 Potential security threat

Since the nature of CIoT device communication is a short burst, AS level attack surface is much less compared to normal UEs which need a sustained connection and complete AS security. For such CIoT devices, if application level security is enabled, encryption may not be a critical need between the UE and the gNB. But to avoid any packet injection or manipulation integrity may be enabled at the radio layer. There is a need to balance the resource availability such as computing power, battery consumption and security threat for CIoT UEs at the radio level. Hence a range of AS security options (encryption vs integrity) need to be supported at the AS layer.

### 5.6.2 Potential security requirements

FFS

## 5.7 Key Issue #7: Key refreshing for protection of small data

### 5.7.1 Key issue details

The 3GPP TR 23.724 [2] contains two key issues on the support of infrequent and frequent small data communication respectively in clause 5.1 and 5.2. Based on the description, the infrequent small data feature is targeted at low complexity, power constrained and low rate UEs, e.g. utility meters, which in some scenarios might be stationary. The frequent small data feature on the other hand is targeted at more active UEs, e.g. tracking devices with an assumed traffic pattern ranging from few transmissions per hour to multiple transmissions per minute.

Assuming that the transmitted small data is protected, these new features would imply infrequent versus frequent usage of the session keys whether for confidentiality or integrity protection. Therefore, an attacker on the air interface sniffing the traffic would have more time versus more protected data to mount a key recovery attack. Nevertheless, it is a safer practise to regularly refresh session keys.

### 5.7.2 Security threats

For the infrequent small data feature, an attacker sniffing the traffic on the air interface has more time in between transmissions to mount a key recovery attack. On the other hand, for the frequent small data, the attacker would have access to more protected small data to mount the same attack. If such an attack succeeds, then the attacker would be able to eavesdrop on the communication or even inject counterfeit small data.

### 5.7.3 Potential security requirements

The system shall support an efficient mechanism for refreshing the session keys.

## 5.8 Key Issue #8: Key and mac size for protection of small data

### 5.8.1 Key issue details

The 3GPP SA2 TR 23.724 [2] contains several references on the expected growth of the number of CIoT devices. The key issues on the support of frequent an infrequent small data features in clauses 5.1 and 5.2 respectively mention that while the data size by device would remain small, the number of devices is expected to grow. It is therefore imperative that the security mechanisms for CIoT can sustain such growth in device numbers.

A poorly chosen small size for protection keys or mac tags, e.g. as a compromise to boost performance, can quickly lead to situations where the key space is depleted. This in turns could lead to more frequent situations of key stream reuse and hash collisions. This would facilitate key recovery attacks and increase the chances for an attacker to breach the security of the system. Observe here that the risk of such attacks would still remain low, if the current sizes of 128-bit protection keys and 32-bit long mac are maintained for CIoT security.

### 5.8.2 Security threats

A poorly chosen small size for protection keys or mac tags, e.g. as a compromise to boost performance, can quickly lead to situations where the key space is depleted. Consequently, this would lead to more frequent situations of key stream reuse and hash collisions. An attacker could exploit these weaknesses to mount efficient key recovery attacks and increase his chances for success. If such an attack succeeds, then the attacker would be able to eavesdrop on the communication or even inject counterfeit small data.

### 5.8.3 Potential security requirements

The size of the security keys shall not be reduced.

## 5.9 Key Issue #9: Protection of NIDD interfaces

5.9.1 Issue details

Non-IP Data Delivery (NIDD) is a part of CIoT EPS optimisations and can be used to deliver unstructured data. NIDD is further defined in TS 23.401 [5] clause 4.3.17.8.1 and in TS 23.682 [6] clause 4.5.14. EPS can deliver the Non-IP data using the Service Capability Exposure Function (SCEF) node which is replaced by the Network Exposure Function (NEF) node in 5GS.

The interface utilized by the NIDD procedures between the NEF and the Application Function (AF) is supposed to transfer data and therefore needs to be properly evaluated.

### 5.9.2 Security Threats

In case the interface used by the NIDD procedures lack confidentiality, integrity and replay protection between authenticated endpoints it will be possible for an attacker to eavesdrop, alter data unnoticed and replay packets.

### 5.9.3 Potential security requirements

The NEF-AF interface shall support confidentiality, integrity, and replay protection.

## 5.10 Key issue #10: User Plane data transmission with Connectionless signalling.

### 5.10.1 Description

This key issue addresses User Plane data transmission with Connectionless signalling solutions which supports infrequent small data transmission. In addition, it also provides improvements in UE TX Power Saving Functions, Overload Control for small data by avoiding CP messages for PDU session set up at every data transmission occurrence.

The Connectionless service also covers the requirement for (Massive) IoT UEs that may move and need to send sporadic (potentially small amount) data: in this case the UE sends data to the 5GC via the user plane path without requiring more signalling in the network (RAN and Core) than the amount of user data to be transferred.

Connectionless service supports a fast switch from IDLE state to a CL-data state where data transfer occurs.

The UE registers to the network and set-up a PDU session that is indicated for CL signalling. When the UE exchanges MM or SM related signalling with the network a N2 connection is set-up. Once the MM or SM transaction(s) are over the N2 connection for the UE is released.

Once the PDU session has been established, the UE is able to send and to receive data without any need to first set-up a connection on N2 or N3. All user plane traffic is carried over an N3 tunnel that can be shared by all active connectionless mode UEs that are currently being served by the same RAN node and the same PDU session type on the same UPF.

### 5.10.2 Potential security threat

Since the RAN node doesn’t use a UE specific security context to protect the transmission of the UE, the Connectionless radio resources of the RAN node could be consumed by UEs which are not authorized for this service. RAN node can be attacked to exhaust all the radio resources.

Unauthorized UEs also may send invalid junk data to the UPF, which might transmit further in to the core network consuming all the bandwidth. Hence it should be possible for the UPF to receive Connectionless data packets only from legitimate UEs already registered for the service with SMF.

The connectionless data from the UE may be manipulated by the man in the middle. If the data is not encrypted, there is no privacy for the data. Also, if the data is not integrity protected, the data may be subject to manipulation.

### 5.10.3 Potential security requirements

It should be possible for RAN node to allow Connectionless service only genuine UEs who have successfully registered for CL service with the SMF.

It should be possible to for the termination pointsto receive the Connectionless data only from legitimately registered UEs for the Connectionless service.

It should be possible for the UE and termination points to encrypt and decrypt the Connectionless data packet with UE specific security keys.

IT should be possible for the UE and termination points to integrity the Connectionless data packet with UE specific security keys.

## 5.11 Key Issue #11: Bidding down attack for NAS based redirection between core networks

### 5.11.1 Key issue details

It is agreed in clause 8.15 in TR 23.724 [9] that core network selection for CIoT could be addressed to use NAS based redirection solution. That is: When a UE triggered registration either in EPC or 5GC network, network may redirect the UE to target system by indication in the NAS layer due to operator policy, e.g. due to roaming agreements, UE's Preferred and Supported Network Behaviour, load redistribution, etc.

However, as shown in Figure 5.10.1-1, when the UE is redirected from 5GC to EPC network, the UE is requested by the network in a Registration Reject message which is sent before NAS SMC and meanwhile the RRC security is not activated. Thus, the UE has bidding down security threat when an attacker forges a registration reject message to the UE to force the UE from 5GC to EPC network.



**Figure 5.10.1-1 Redirection from 5GC to EPC network**

When the UE redirects from 5GC to EPC network, some security enhancement feature in 5G may be not available anymore, e.g. SUPI protection, initial NAS protection, etc. The UE privacy may be exposed.

### 5.11.2 Security threats

Attacker may forge a registration reject message to the UE to force the UE redirect from 5GC to EPC network, may lead unavailable of 5G security enhancement feature, e.g. SUPI protection, initial NAS protection, etc. The UE privacy may be exposed.

### 5.11.3 Potential security requirements

5GS shall protect the redirection message.

## 5.12 Key Issue #12: Privacy protection of new parameters for CIoT included in NAS message

### 5.12.1 Key issue details

The 3GPP TR 23.724 [2] has recommended many solutions for normative work where many of the solutions implies that new parameters for CIoT will be included by the UE in the NAS message to the AMF. Some of these new parameters for CIoT may require encryption if they are privacy sensitive. Each new parameter introduced by the various solutions needs to be checked whether it can be sent in clear text or not.

For example, in the recommended solution #9 in 3GPP TR 23.724 [2] for normative work, the UE may indicate preference for MICO mode and optionally request and indicate a preferred Active Time value to the AMF during an initial Registration or Registration Update procedure.

### 5.12.2 Security threats

Threat to be protected against is: re-identification of UE by exchanged parameters and associated UE behaviour.

### 5.12.3 Potential security requirements

TBD

## 5.13 Key Issue #13: Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC

### 5.13.1 Key issue details

In order to meet low-power consumption requirement, CIoT UE does not support measurement report, so, handover is not supported for mobility because the source RAN has no reference to trigger handover. Instead, RRC Re-establishment procedure is used to support mobility.

RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC is used to support mobility handling in NB-IoT CP optimisations. The procedure has been introduced in LTE in clause 7.4.4 in TS 33.401 [2]. It would lead to a functionality gap between 5GC and EPC for mobility handling in NB-IoT CP optimisations if RRC Connection Re-establishment is not supported or does not work properly in 5GC.

Since AS security is not activated for NB-IoT CP optimisations solution, the UE and the RAN cannot authenticate each other using AS security in Re-establishment procedure. In TS 33.401 [2], current solution uses NAS protection for RRC Re-establishment Request message using S-TMSI for RAN to find the MME for doing UE verification, and uses NAS protection for RRC Re-establishment message for the UE to do MME verification.

If the same procedure is introduced in 5G, NAS protection for RRC Re-establishment procedure is expected to be used. Therefore, the following two issues shall be considered for the RRC Re-establishment procedure using NAS protection to work:

1. If the same security parameters (ul-NAS-MAC and ul-NAS-Count) as in EPS are used, currently there is no sufficient space to carry the 5G S-TMSI and thus a truncated 5G S-TMSI (e.g. 40 bits) may need to be defined.
2. Since KAMF key separation functionality have been defined in TS33.501 [3] and when this feature is enabled, there is a possibility for the UE and the NG-RAN to go out of synch with respect to the used NG-RAN security keys during the RRC Re-establishment procedure.

NOTE: The definition of the truncated 5G S-TMSI is pending on SA2/CT4 discussion.

### 5.13.2 Security threats

If there is no secure mechanism for RRC Re-establishment Request message for the control plane for NB-IoT, it will be possible for an attacker to tamper with and replay RRC signalling, which may lead to forgery of real UE and network identity.

### 5.13.3 Potential security requirements

The 5GS shall support a security mechanism for the RRC Re-establishment procedure for the control plane for NB-IoT.

## 5.14 Key issue #14: Preventing User Plane Botnet Attacks from Improper CIOT Device Usage

### 5.14.1 Description

A vulnerability posed to CIOT devices is the ability for them to be exploited by botnets and other automated distributed threats. Once compromised, a CIOT device can be used to attack any other system on the internet, often times there is nothing limiting the functionality of a compromised CIOT devices to be used in ways the manufacture did not intend. These attacks may take place on user plane or on signalling plane. This key issue deals with user plane, as signalling plane attacks are already addressed in key issue #4. The ability for the network to be aware what type of access and network functionality a CIOT device requires to operate properly enables the network to block any behaviour outside of that scope. Constraining the communication abilities of exploited CIOT devices reduces the potential for the devices to be used in these types of attacks.

### 5.14.2 Potential security threat

Compromised CIOT devices may be directed to perform operations the manufacturer did not intend. While the capabilities of individual CIOT devices are often limited, the capabilities of CIOT-based botnets in aggregate may be sufficient to cause major network and enterprise outages.[4] Misuse of compromised IoT devices has been a critical component in recent automated botnet attacks, specifically distributed denial of service attacks.

### 5.14.3 Potential security requirements

5GS shall be able to establish the expected user plane communication behaviour of CIoT devices to mitigate potential DDOS attack.

## 5.15 Key Issue #15: Protection of UE capability transfer for UEs without AS security

### 5.15.1 Key issue details

GSMA sent an LS to SA3 and RAN2 in [17] describing the vulnerability in current 3GPP RRC specifications for the UECapabilityEnquiry procedure. Tampering of UE capabilities by MITM attacker on the radio surface was possible as Rel 15 TS 33.501 specification was allowing UE capability Enquiry to occur before RRC security establishment. MITM attack can cause a denial of service attack, as described in the [17].

“This exposes the UE capabilities to tampering by a man-in-the-middle attacker on the radio interface, which can result in degradation of service, e.g., downgrading the UE’s maximum throughput. Since the UE capabilities are persistently stored in the network, the impact of the attack can last for weeks, or until the UE is power cycled. Such attacks can have a particularly high impact on unattended IoT devices. The researchers have demonstrated the feasibility of the attack using low-cost equipment.”

The researchers describe related vulnerabilities in 3GPP specifications for the capability transfer procedures in [18]. The Device identification is based on the differential analysis of the capabilities that are obtained from a UE. With the reference model, baseband vendors, OS developers or device manufacturers are all possibly detected. The attackers may determine potential vulnerabilities applicable to the identified device, which has potential security threats.

“*The secondary goal of this attack is to determine potential vulnerabilities applicable to the identified device. Precisely, MNmap can be supplemented with vulnerability information from the external sources such as vulnerability databases from baseband vendors (Huawei [25], Qualcomm [29]), OS developers (Google [19], Apple [16]) and device manufacturers (Samsung [33]) and perform targeted attacks. Further, these device fingerprints can be combined with the permanent identifier IMSI to track subscribers. While 5G prohibited the plaintext transmission of IMSI in any situation [12, 14], fingerprinting of a device and user is still possible when the device-type information is unique among the nearby devices.”*

To address the issue, SA3 specified security protection of the RRC UE capability transfer procedure in 33.501 [8]. The fundamental requirement of the protection is that UE supports AS security. However, there is a type of CIoT devices that only support control-plane optimization. Such devices do not support AS security for UE capability transfer. For those devices, it is necessary to develop a security solution that enables network to verify the UE radio capabilities provided by the UE.

### 5.15.2 Security threats

Attacker may inject false UE radio capabilities for CIoT UEs that only support CP optimization. This may cause unexpected damage to those CIoT UEs, including but not limited to, service downgrade, denial of service, battery exhaustion.

The following are some of the examples for Radio capability that are transferred in clear text and have the potential for hijack by MiTM adversary. MiTM adversary can alter UE capability information sent by the UE, resulting in a denial of service and battery degradation. Storing the UE capability at AMF for a concise period will not solve the following issues.

* UE-Category-NB-r13: If altered and set to 0, the network will discard and release the UE.
* SupportedBandList-NB-r13 and FreqBandIndicator-NB-r-13: If MITM changes the band to value which is not supported by UE, the UE may become dysfunctional and never be able to connect to the network.
* Multicarrier-r13: If altered and set to disabled, then every UE will use a single carrier and will result in congestion of the network.
* powerClassNB-20dBm: If altered and set to powerClassNB-14dBM, then low power and low complexity devices don’t support this 20 dBm power class, then it may impact uplink transmit power control.
* PDCP supportedROHC-Profiles-r13: If altered and set to enabled, it may cause much overhead for low complexity devices.
* AcceStratumRelease-NB-r13: If set to Rel 15 or any future release, then the network thinks UE supports many new features of Rel-15 or any future release.

### 5.15.2 Potential security requirements

The system shall support to mitigate the effects of handling unprotected UE radio capability for UEs without AS security.

## 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: Security Solution for small data transmission via NAS signaling

### 6.1.1 Introduction

This solution addresses key issue #2: Integrity protection of small data and key issue #3 : Encryption of small data .

The key issue proposes to integrity- and confidentiality- protect small data for security data transmission solutions in TR 23.724. There is a set of solutions which transfer small data via NAS signalling, e.g. solution 1, solution 2, solution 3, solution 4, etc. All of these solutions have common features:

1. For MO data transport, the MO small data is included in NAS PDU, and is transferred in initial NAS message;
2. For MT data transport, the MT small data is also included in NAS PDU, and is transferred in DL NAS message.

The differences of these solutions, e.g. whether AMF delivers data to UPF via vSMF or directly, whether NAS PDU includes path information, are not related to security.

So, from security aspect, since the small data is transferred in initial NAS message or DL NAS message, the proposed security solutions are very similar with current NB-IoT CP solution in LTE. So, this solution proposes to reuse security solution of current NB-IoT CP solution.

### 6.1.2 Solution details

For MO data transport,

1. The small data payload in initial NAS message shall be ciphered. The partial cipher mechanism defined in clause 8.2 of TS 33.401 [7] can be reused to protect the MO NAS PDU in the initial NAS message.
2. The small data payload in initial NAS message shall be integrity protected. The small data payload shall be integrity protected because the small data payload is already included in initial NAS message.

For MT data transport,

1. The small data payload shall be ciphered. The small data payload shall be ciphered because the small data payload is already included in DL NAS message.
2. The small data payload shall be integrity protected. The small data payload shall be integrity protected because the small data payload is already included in DL NAS message.

Possible security solutions for how to handle small data included in initial NAS message at AMF reallocation are given in other solutions, e.g. solution #5 in clause 6.5, solution #9 in clause 6.9 and solution #10 in clause 6.10.

### 6.1.3 Evaluation

## 6.2 Solution #2: Efficient integrity protection for frequent small data transmissions

### 6.2.1 Introduction

This solution addresses the key issue #1 "Efficient frequent small data transmissions" and the key issue #2 "Integrity protection of small data". This solution reduces the overhead of MAC-I (Message Authentication Code-Integrity) included in the small data when integrity protection is applied in the UP. The relative overhead of MAC-I is high as the payload size is small, and thus it decrease the effective user data throughput. The proposed solution decreases the overhead by calculating and transmitting one MAC-I for multiple small data.

### 6.2.2 Solution details

As shown in figure 6.2.2-1, depending on the traffic load, MAC-I is calculated for the set of N data as a single unit. All data 1 through N are input to the integrity function along with security key and other parameters such as counters or an algorithm identifier. Then each of data 1 to data N is sent to the receiver individually. The value of N can be defined as a fixed value or dynamically adjusted depending on the various circumstances (e.g. traffic type, traffic load).

Figure 6.2.2-2 illustrates this solution. Data 1 through N-1 are sent without MAC-I, and MAC-I is inserted in the last data unit (i.e. data N) only. This MAC-I represents the integrity of the entire series of data 1 through N instead of individual data having its own MAC-I.

In order to indicate whether the transmitted data includes the MAC-I or not at the receiver side, one of the reserved bits (bit E in the figure) in PDCP header is used. The value of E=0 is set when the MAC-I is not included (i.e. data 1 through N-1), and the value of E=1 is set when the MAC-I is included (i.e. data N only). The receiver side stores the data 1 through N and apply the integrity protection check using the content in MAC-I for the entire series of data 1 through N.

Furthermore, another reserved bit (bit P in the figure) indicates the priority of the payload content. The transmitter sets the values of 0 and 1 when the priority is low and high, respectively. If the received PDCP message contains P=1, then the receiving side is required to verify the integrity of the message by checking against the MAC-I. If the received PDCP message contains P=0, then the integrity checking of the received message is not mandatory and is left up to the receiver side by taking into account its operating condition such as the data rate or its processing load. This handling allows the receiving side to further save the processing power. The P value is the same for entire series of the data 1 through N.

The value of N may be determined in the network and the UE by mechanism such as: 1) static configuration, 2) dynamic negotiation between the gNB and the UE, 3) include it in the UP packet itself, etc.

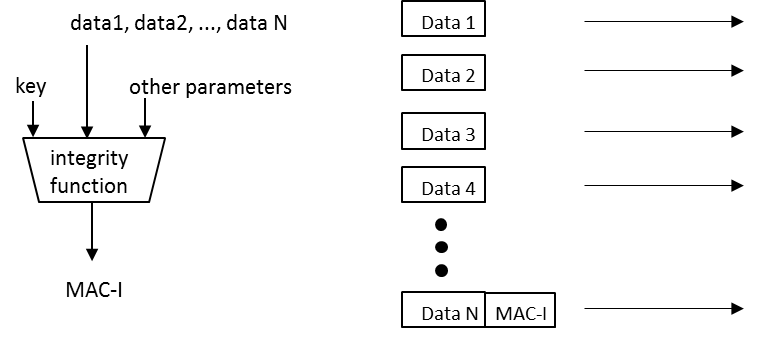


Figure 6.2.2-1 Efficient integrity protection for small data transmission

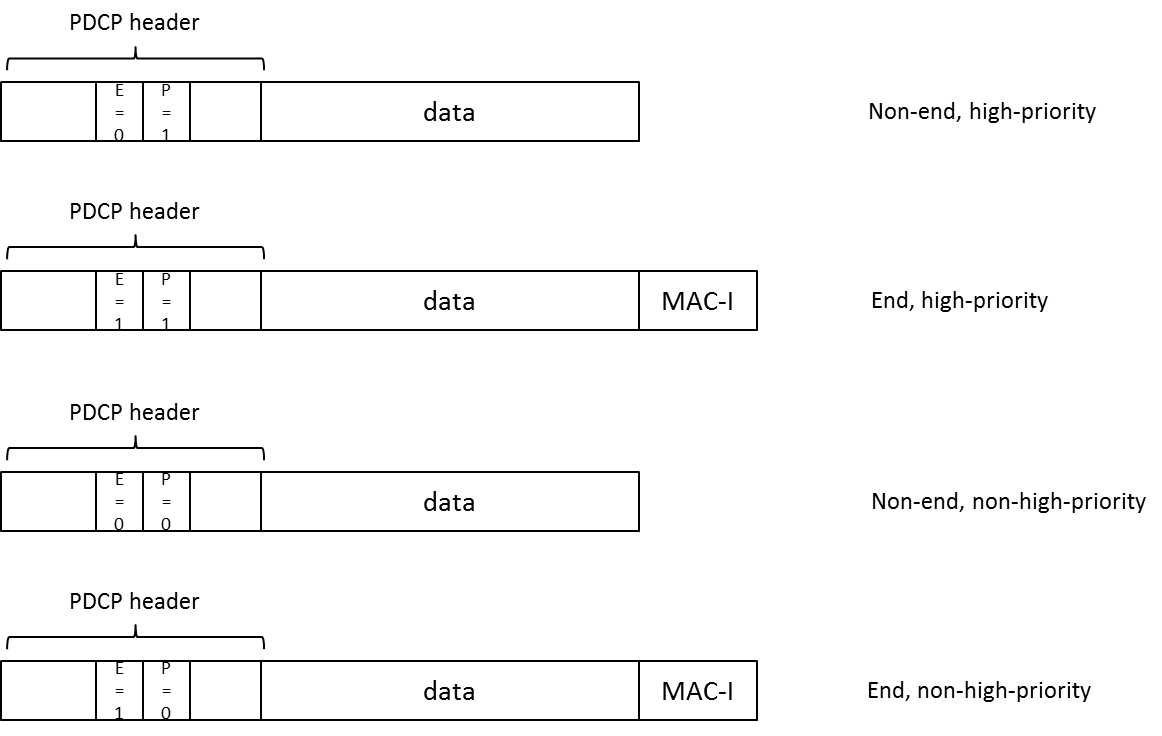


Figure 6.2.2-2 PCDP PDU format for efficient integrity protection

### 6.2.3 Evaluation

This solution addresses the key issue #1 and #2.

This solution reduces the overhead caused by MAC-I calculation by aggregating multiple N PDCP frames into a single integrity protected unit. Depending on the value of N, the calculation of MAC-I on the transmitting side and checking of MAC-I on the receiving side can be significantly reduced.

This solution implies that, on the receiving side, all data 1 through N needs to be received and buffered before the integrity check can be applied. Also, all data 1 through N need to be discarded if the integrity check fails. If the re-transmission of N PDCP frames becomes necessary, it can negatively impact the overall throughput and effective data rate. The performance impact can be determined by the choice of value N.

Furthermore, the priority bit in the PDCP header allows the device to determine whether to verify the receivedMAC-I or not depending on its operating condition. In this case, the saving of processing resource can be achieved for the price of not verifying the integrity of the received PDCP frames.

To ensure backward compatibility with legacy UEs, new mechanism in Uu interface signalling is required to communicate the support of this functionality in both the UE and the network. The exact definition for this mechanism falls in RAN2's purview and thus out of scope of this document.

Editor's Note: Evaluation against other key issues is needed.

## 6.3 Solution #3: Security solution for MO SMS at AMF re-allocation

### 6.3.1 Introduction

This solution addresses key issue #2: Integrity protection of small data and key issue #3: Encryption of small data in this TR.

In this solution, small data is included in a MO SMS. This security solution proposes an optimized NAS signalling solution for sending small data in a MO SMS. The MO SMS is included in an initial NAS message (e,g, Registration Request) whenever the UE has a valid 5G security context. This solution assumes that the UE has information about whether the target AMF supports MO SMS or not. This security solution for small data proposes to re-use NAS security, with the enhancement of deriving an additional encryption key, i.e. a new one-time encryption key, for encryption of MO SMS (including the small data) included in initial NAS signalling messages.

The motivation for introducing the new one-time encryption key, is that when a target AMF receives the initial NAS message from the UE, then the target AMF forwards the whole initial NAS message to the source AMF who performs the integrity check of the initial NAS message. If the integrity check of the whole initial NAS message is successful, then the source AMF releases the 5G security context to the target AMF. Besides perfoming the integrity check, the source AMF does not need to act on the initial NAS message, e.g. by decrypting the small data and forwarding it to the target AMF. Also, if the source AMF has performed horizontal Kamf derivation of the current Kamf, then the source AMF will not forward the current Kamf key, current NAS keys etc. to the target AMF. The source AMF will only forward the new Kamf key to the target AMF. The target AMF does not have the NAS encryption key which the UE used to encrypt the MO SMS containing small data.

### 6.3.2 Solution details

#### 6.3.2.1 MO SMS included in initial NAS message

This security solution describes how to protect MO SMS in initial NAS message. The following figure shows a MO SMS delivered from the UE using initial NAS message at AMF re-allocation.

It is expected that MO SMS sent over 5G will be both integrity protected and ciphered using NAS security.

This security solution proposes that the UE and the AMF derive a new security key (one-time key) from the current 5G security context for the encryption of the MO SMS included in the initial NAS message. This new one-time key could be derived from the current KAMF key in use. The new one-time key is different to current KNASenc key. In order to preserve the backward security mechanism, this one-time key must be used only once per initial NAS message. The remaining NAS messages (downlink and uplink) are protected using the usual NAS keys from the active NAS security context.

A detailed description of the steps is given below.



**Figure 6.3.2.1-1: One-time encryption key protecting MO SMS in initial NAS message**

The steps are as follows:

1. It is assumed that the UE has earlier registered and established NAS security and then went back to CM-IDLE mode e.g. due to inactivity.
2. The UE decides to send a MO SMS and initiates the establishment of a NAS connection with the network by initiating an initial NAS message. This initial NAS message could be e.g. a Registration Request due to UE mobility to another tracking area when AMF reallocation may take place. The UE must construct an initial NAS message that is integrity protected by the already established 5G NAS security context. For the encryption of the IE containing the MO SMS, the UE derives a new one-time encryption key, for example from the current KAMF key in the 5G NAS security context and the UL NAS COUNT and encrypt the MO SMS with the new one-time encryption key.
3. Upon reception of the initial NAS message, the target AMF retrieves the UE context from the last serving AMF (i.e. source AMF). The context request message to the source AMF includes the temporary identifier 5G-GUTI and the whole received initial NAS message from the UE.
4. The source AMF verifies the integrity of the received initial NAS message using its stored 5G NAS security context. If the verification of the integrity check is successful, the source AMF shall release the 5G security context to the target AMF. In addition, the source AMF derives a new one-time encryption key from the current KAMF key in the current 5G NAS security context and the UL NAS COUNT and delivers the new one-time encryption key to the target AMF. The derivation of the new one-time encryption key is performed by the source AMF regardless whether source AMF performs horizontal KAMF derivation or not.
5. If source AMF performs horizontal KAMF derivation then the source AMF delivers the new KAMF key together with the new one-time encryption key (derived from the old KAMF key to the target AMF), otherwise the source AMF delivers the current KAMF key together with the new one-time encryption key to the target AMF.
6. The target AMF uses the one-time encryption key received from the source AMF to decipher the ciphered IE containing the MO SMS included in the initial NAS message.
7. The target AMF forwards the MO SMS to the SMSF and deletes the one-time encryption key.
8. The target AMF and UE proceeds as described in step 6 and onwards in clause 4.2.2.2.2 in TS 23.502 [15].

### 6.3.3 Evaluation

The proposed solution fulfils the potential security requirements of KI#2 and KI#3. The outstanding issue is how the feature support is negotiated between the UE and the target AMF at AMF re-allocation. MO SMS included in NAS message was introduced already in 5G system in Rel-15 in TS 23.501 [10] and TS 23.502 [15] as an optional feature in UE and AMF. In Rel-15, the UE and AMF negotiates the support of MO SMS by the UE including "SMS over NAS supported" in Registration Request to the AMF and an AMF supporting this feature is responding back to the UE by including "SMS over NAS allowed" in Registration Accept. The UE stores this information in its UE context.

In Rel-15, the UE is not allowed to include MO SMS into Registration Request message. When the UE wants to send MO SMS then the UE is already registered in the AMF and the negotiation has already taken place between the UE and AMF before the UE includes the MO SMS into a NAS message. Unless the support of "SMS over NAS allowed" and "MO SMS included into Registration Request" are broadcasted in system information in Rel-16, the UE has no knowledge of whether the target AMF Rel-16 supports MO SMS included into Registration Request beforehand at AMF change.

## 6.4 Solution #4: Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT)

### 6.4.1 Introduction

This solution addresses key issue #2: Integrity protection of small data, key issue #3: Encryption of small data in this TR.

This security solution address solution 19: 5GS UP Optimization for Infrequent Small Data Transmission in SA2 TR 23.724 [2]. This solution is to optimize small data transmission for the UEs from CM-IDLE mode. It enables transfer of user plane data without need for the Service Request procedure. According to solution 19 in SA2 TR 23.724 [2], it is proposed to keep AS context in the NG-RAN including information the UPF connection and relevant QoS flow(s) to be used for the connection, even when UE moves into CM-IDLE. When UE resumes the connection, the NG-RAN uses the information to activate DRB, AS security and User Plane connectivity over N3 for the small data packet delivery to the UPF.

In EPS/LTE Rel-15, early data transmission (EDT) feature was added to the RRC Connection Resume/Suspend procedures in eNB as specified in TS 33.401 [7]. Uplink user plane data is included as early data transmission with the RRC Connection Resume Request (msg 3). As described in TS 33.401 [7], the UE and the target eNB uses the newly derived KUPenc for ciphering/deciphering of the UL EDT data in PDCP layer in the RRC Connection Resume Request message, and user DL data (if included) in PDCP layer in the RRC Connection Suspend or RRC Connection Resume message.

Note: The current solution in TS33.401 does not provide integrity protection of the EDT UL UP data included during the RRC Resume procedure.

This solution proposes to re-use the security solution for RRC Suspend and Resume procedures with EDT as defined in EPS/LTE Rel-15 in clause 7.2.11.3 in TS 33.401 [7] for E-UTRA connected to 5GC, with the following enhancements:

* . The UL UP data is integrity protected while being transmitted over SRB0 during the RRC Resume procedure as detailed in this solution.

### 6.4.2 Solution details

#### 6.4.2.1 UL data transmission from CM-IDLE (SUSPEND) with Early Data Transmission to old eNB

The following figure shows a single MO small data delivered from the UE using Early Data Transmission.



**Figure 6.4.2.2-1: Single MO data Transmission using and Early Data Transmission (EDT) with UL UP IP**

Figure 6.4.2.2-1 shows the following steps:

1. The UE calculate the hash of UL UP data as follows:
   1. Over each PDCP PDU, HASHUE-PDU(i) of the UL UP data.
   2. When the UE calculate the ShortResumeMAC-I, the UE uses a predefined order based on the increasing DRB-ID and PDCP SN of the PDCP PDUs when using the Hashes of the PDCP PDUs as input parameters to the ShortResumeMAC-Input; thus the HASHUE-PDUs are protected by the ShortResumeMAC-I token, e.g., ShortResumeMAC-Input “Source (C-RNTI+PCI) + Target Cell ID + HASHUE-PDU(1) + HASHUE-PDU(2) ”
2. The UE sends the UL small data included as UL EDT (Early Data Transmission) with the RRC Connection Resume Request (msg 3) on SRB0 and hence it is integrity protected. The UE includes information to be used for context identification and re-establishment in the RRC Connection Resume Request message: The Resume ID and a ShortResumeMAC-I.
3. The eNB identifies the UE context, validate the ShortResumeMAC-I, and if successful decrypt the UL UP data.
4. The eNB forward the UL UP data to the UPF as described in TS 23.724 [2].
5. The eNB derives the new Krrcint and Krrcenc to protect and send the RRCConnectionRelease message which include an indication of suspend. The RAN may immediately after step 3 suspends the RRC connection (to minimize UE power consumption) as described in TS 23.724 [2].

6. UE and RAN remain suspended as described in TS 23.724 [2].

#### 6.4.2.2 UL UP EDT from RRC SUSPEND to new eNB

Since the new eNB does not have the UE context, the new eNB sends a RETRIEVE UE CONTEXT REQUEST message to the old eNB. The new eNB include the UE I-RNTI, the ShortResumeMAC-I, and the UL UP data for the old eNB to calculate the HASHUE-PDU(s) as done by the UE and validate the ShortResumeMAC-I using the old Krrcint. If successful, the old eNB sends a RETRIEVE UE CONTEXT RESPONSE message with the UE context included and the new KeNB\* or NH.

After the new eNB receives the RETRIEVE UE CONTEXT RESPONSE message, it decrypts the UL UP data and forward it to the UPF. In addition, the new eNB derive the new Krrcint and Krrcenc to protect the RRCConnectionRelease message which include an indication of suspend.

#### 6.4.2.3 Connection Suspend procedure using the Early Data Transmission (EDT) feature

This procedure is used by the RAN to suspend the connection if 5GS UP Optimization is supported as described in solution 19 in TS 23.724 [2].

### 6.4.3 Evaluation

It has been identified that there is a potential problem with this security solution as the target/new ng-eNB (for eMTC) does not have the UE context when it receives the RRC Connection Resume Request message from the UE and is therefore not able to decode the PDCP PDUs because the target/new ng-eNB (for eMTC) does not know the RLC and PDCP configurations. The MAC configuration can be assumed to be default/cell specific configuration for first UL transmission as target/new ng-eNB (for eMTC) needs to process the first MAC PDU before the UE AS context is available.

An attacker can bid down the application of the integrity protection by, for example, acting as a MitM between the UE and network and rejecting the resume request. This results in the UE transitioning to idle and then connecting to send the data. The data will be sent without integrity protection and hence the adding integrity protection to the EDT data has been bid-down.

In LTE including eLTE (LTE UE connected to 5GC), integrity protection of user plane data is not supported. Therefore, any solution requires a change in UE behavior and would not be compatible with legacy eNBs. Today RRC calculates the *shortResumeMAC-I* independent of PDCP data PDU and includes it in *RRCConnectionResumeRequest* message. In this solution, RRC would need to delay the *shortResumeMAC-I* calculation until PDCP data PDU(s) is ready and new AS keys are derived and integrity protection and ciphering in the PDCP layer is performed. It is because the HASH code needed in the calculation of *shortResumeMAC-I* is calculated from the PDCP PDU.

## 6.5 Solution #5: Security solution for small data included in initial NAS signalling at mobility

### 6.5.1 Introduction

This solution addresses key issue #2: Integrity protection of small data and key issue #3: Encryption of small data in this TR.

As defined in TS 23.401 [5], the Control Plane CIoT EPS optimisation to send small data over NAS was added in EPS/LTE Rel-13. A NB-IoT UE could include small data in NAS signalling (DoNAS) to the MME. To support DoNAS was optional in MME but mandatory in NB-IoT UE. The NB-IoT UE is allowed to include DoNAS into NAS signalling messages as Service Request message, Uplink NAS Transport message, but not in Attach Request message and Tracking Area Update Request message as the NB-IoT UE had no knowledge of whether the target MME supported Control Plane CIoT EPS Optimization.

This security solution proposes an optimized NAS signalling solution for sending small data. This security solution for small data proposes to re-use NAS security, with the enhancement of deriving an additional encryption key, i.e. a new one-time key, for encryption of small data included in initial NAS signalling messages.

The motivation for introducing the new one-time encryption key, is that when a target AMF receives the initial NAS message from the UE, then the target AMF forwards the whole initial NAS message to the source AMF who performs the integrity check of the initial NAS message. If the integrity check of the whole initial NAS message is successful, then the source AMF releases the 5G security context to the target AMF. Besides perfomring the integrity check, the source AMF does not need to act on the initial NAS message, e.g. by decrypting the small data and forwarding it to the target AMF. Also, if the source AMF has performed horizontal Kamf derivation of the current Kamf, then the source AMF will not forward the current Kamf key, current NAS keys etc. to the target AMF. The source AMF will only forward the new Kamf key to the target AMF. The target AMF does not have the NAS encryption key which the UE used to encrypt the small data.

### 6.5.2 Solution details

This security solution describes how to security protect small data in initial NAS message.

The following figure shows the scenario at mobility when UE includes a small data packet in the initial NAS message and an AMF change takes place.

This solution assumes that the UE has information about whether the target AMF supports small data in NAS or not.

It is expected that small data included in initial NAS message sent over 5G will be both integrity protected and ciphered using NAS security.

This security solution proposes that the UE and the AMF derive a new encryption key (one-time key) from the current 5G security context for the encryption of the small data included in the initial NAS message. This new one-time key could for example be derived from the current KAMF key in use. The new one-time key is a different key compared to current NAS encryption key i.e. KNASenc key. In order to preserve the backward security mechanism, this one-time key must be used only once per initial NAS message so that it can be safely be handed over to a new AMF, in mobility events, without compromising the security of protected IE’s sent earlier by the UE to different AMF’s.

This solution would ensure that the source AMF would not need to decrypt the encrypted IE’s received in the initial NAS message (e.g. Registration Request message). Instead the source AMF derives the new one-time key from the current 5G security context and provides the new one-time key to the target AMF, and then the target AMF can decrypt the encrypted IE’s received in the initial NAS message (e.g. Registration Request message) using the one-time key. After the decryption, the target AMF deletes the one-time key.

A detailed description of the steps is given below.



**Figure 6.5.2.1-1: One-time key protecting small data included in initial NAS message**

The steps are as follows:

1. It is assumed that the UE has earlier registered and established NAS security and then went back to CM-IDLE mode e.g. due to inactivity.
2. The UE decides to send a small data packet and initiates the establishment of a NAS connection with the network by initiating an initial NAS message. The UE must construct an initial NAS message that is integrity protected by the already established 5G NAS security context (i.e. current KNASint key). For the encryption of the IE containing the small data, the UE derives a new one-time encryption key, for example from the current KAMF key in the 5G NAS security context and the UL NAS COUNT, and encrypt the IE containing small data with the new one-time encryption key. The new one-time key is a different key compared to current NAS encryption key i.e. KNASenc key.
3. Upon reception of the initial NAS message, the target AMF retrieves the UE context from the last serving AMF (i.e. source AMF). The context request message to the source AMF includes the temporary identifier 5G-GUTI and the whole received initial NAS message from the UE.
4. The source AMF verifies the integrity of the received initial NAS message using its stored 5G NAS security context (i.e. current KNASint key). If the verification of the integrity check is successful, the source AMF shall release the 5G security context to the target AMF. In addition, the source AMF derives a new one-time encryption key from the current KAMF key in the current 5G NAS security context and the UL NAS COUNT and delivers the new one-time encryption key to the target AMF. The derivation of the new one-time encryption key is derived from the current KAMF key by the source AMF regardless whether source AMF performs horizontal KAMF derivation of the current KAMF key or not.
5. If source AMF performs horizontal KAMF derivation then the source AMF delivers the new KAMF key together with the new one-time encryption key (derived from the old KAMF key to the target AMF), otherwise the source AMF delivers the current KAMF key together with the new one-time encryption key to the target AMF.
6. The target AMF uses the one-time encryption key received from the source AMF to decipher the ciphered IE containing the small data included in the initial NAS message. The target AMF forwards the small data packet to the SMF or UPF and deletes the one-time encryption key.
7. The target AMF forwards the UL small data to the SMF or the UPF.
8. The SMF or the UPF may forward DL small data to the target AMF.
9. The target AMF uses the one-time encryption key to cipher the IE for DL small data transfer.
10. The target AMF and the UE proceeds as described in step 6 and onwards in clause 4.2.2.2.2 in TS 23.502 [15]. The target AMF forwards the IE for DL small data transfer in a downlink NAS message.

### 6.5.3 Evaluation

The proposed solution fulfils the potential security requirements of KI#2 and KI#3.

The outstanding issue is whether the UE can include small data in Registration Request in 5G Rel-16. Small data included in NAS messages, will be a new feature in Rel-16 as small data was not supported in 5G Rel-15. It’s not concluded whether a similar approach will be taken in 5G CIoT as in 4G CIoT, where the broadcast system information provides information about support of Control Plane CIoT EPS Optimisation. If yes, then this information may be used by the UE to determine whether Control Plane CIoT 5GS Optimisation is supported in 5GC.

## 6.6 Solution #6: Detecting and handling signalling overload due to Malicious Applications on the UE

### 6.6.1 Introduction

This solution addresses Key Issue #4: Signalling overload due to Malicious Applications on the UE.

A large number of UEs performing similar actions at the same time can easily lead to a signalling attack on the network. If such an attack persists and isn’t dealt with appropriately it brings a risk for other users of the network. As such, mitigating measures should be designed to protect the networks against such attacks.

For this solution, it is assumed that the malicious behaviour on the UE is the result of an attacker having access to the Application on the UE which it can instruct to make certain requests to the network. An attacker could have obtained this access through the over the top service and could for example instruct the UE to set up dedicated bearers or request access to certain network slices. Such procedures could lead to exhaustion of resources in both the radio and the core network, which would lead to denial of service or service degradation for other users of the network.

An important assumption of this key issue is that the UE part that is responsible for executing the radio instructions remains untouched. Also, it is assumed that the USIM is not compromised. Hence, the solution has limited applicability: not every malicious UE can be controlled.

### 6.6.2 Solution details

#### 6.6.2.1 Architecture

This solution consists of a network data analytics function and logic in the network and a security function and logic in the UE.

The network side of the solution is based on the 3GPP network data analytics function NWDAF as specified in TS 23.288 [12], and in particular on the functionality to collect data and to report on abnormal UE behaviour as specified in TS 23.288 [12], clause 6.7.5.

The NFs can receive information about abnormal UE behaviour is two ways according to the principles of network data analytics:

a) the NF can subscribe to analytics data and receive a notification containing this data, or

b) the NF can request analytics data and receive it in the response.

So, whenever the NF is under high load, the NF can contact the NWDAF for analytics data. The request may include a list of UEs, such that the NWDAF can provide the corresponding analytics data for this list of UEs. The information flow between the NF and the NWDAF can take one of two forms depending on the mode of operation a), or b) above.

For case a) the messages exchanged between NF and NWDAF are:

- Nnwdaf\_AnalyticsSubscription\_Subscribe;

- Nnwdaf\_AnalyticsSubscription\_Notify.

For case b) the messages exchanged between NF and NWDAF are:

- Nnwdaf\_AnalyticsInfo\_Request;

- Nnwdaf\_AnalyticsInfo\_Response.

After reception of the analytics data on abnormal UE behaviour, the NF can decide on the appropriate action.

The UE side of the solution assumes a security function (UESF) and logic in the UE that is protected against malware that may have infected Applications on the UE. The security function can interact with the network and receive security instructions from the network.

The architecture of the UE is as depicted in Figure 6.6.2.1-1. As described in TS 23.002 [16] it is composed of a Mobile Equipment (ME) domain and a UICC domain, where the ME Domain is subdivided in one or more Terminal Equipment (TE) and Mobile Termination (MT) components. For the purpose of this solution, the TE is the part of the UE containing the user applications that are susceptible to infection by malware. The MT is the part of the UE that is protected against infection by malware. In this solution the MT itself is comprised of a UE security function (UESF) which is capable of controlling the communication between the TE and the MT and thereby limiting the impact on the network of misbehaving user applications in the TE.



Figure 6.6.2.1-1: User device architecture showing the proposed UE security function inside the UE

The UESF is assumed to be provided with specific security instructions via the method described in clause 6.6.2.2 in case the network detects that the user device is misbehaving. Examples of security instructions are:

* The user device is not allowed to download from a certain IP address, or from a certain set of IP addresses;
* The user device is not allowed to contact the network for the next x minutes;

NOTE: The network is assumed to have a maximum time duration (e.g. 60 minutes) that the user device is not allowed to contact the network. Hence it does not instruct the user device to not contact the network for more than this maximum time duration.

* The user device will be limited to y MB/s for the next z minutes.

Some security instructions can resemble existing functionality in 3GPP, e.g. UE policies or back-off timer functionality, but this solution proposes to use the same uniform approach for providing these instructions with the intention that they are handled by the same UE security function.

#### 6.6.2.2 Procedures

The procedure here is described for the AMF but can easily be changed for another NF.

In this case, the AMF has requested analytics data on a (set of) UEs. The analytics data states that a particular UE has been generating a signalling overload (e.g. as part of DDOS attack), and that this UE should be provided with security instructions (e.g. to lower the signalling load or stop signalling for a certain period. The UE is provided with security instructions using the mechanism of the UE Configuration Update procedure specified TS 23.502 [15]. The flow can look as follows:



Figure 6.6.2.2-1: Signalling overload handling using UE Configuration Update procedure

1. The AMF requests analytics data from the NWDAF.

2. The NWDAF responds to the AMF with analytics data, reporting that a particular UE is acting abnormally.

3. The AMF decides that the reported UE needs to be provided with security instruction (e.g. to lower its signalling load or to back-off during a certain period).

4. The AMF sends security instructions to the MT using the UE Configuration Update-Command.

5. The MT sends the received security instructions to the UESF.

6. The UESF processes the received security instructions.

7. Optionally the UESF provides an acknowledgement of the received security instruction to the MT.

8. Optionally the MT sends a UE Configuration Update Complete message to the AMF indicating the result of the processing of the security instructions.

NOTE: As an alternative information flow the AMF can also subscribe to analytics data and get notified by the NWDAF. This would alter steps 1 and 2 above, but this does not change the remainder of procedure as expressed in steps 3 to 8.

### 6.6.3 Evaluation

Benefit of this solution is that it provides a uniform way to provide a UE with security instructions based on an existing method for providing information to the UE.

Benefit of this solution is that is allows dedicated security functionality to be embedded in the MT part of the user device. It also allows for extensibility of the set of security instructions that can be provided.

Drawback of this solution is that it requires UEs to be enhanced with new security functionality which is tamper-proof, and it requires the addition of security instructions to the UE Configuration Update procedure. The solution does not apply to UEs without this additional functionality and without the updated procedure.

## 6.7 Solution #7: Procedure for protecting gNB from RRC resume and RRC Re-establishment DoS attack

### 6.7.1 Introduction

This solution addresses key issue #5.

The following describes the attack of misbehaving or compromised UE using RRC Resume and/or RRC Re-establishment procedure：

* For the RRC resume procedure, the attack may look like the following:

1. An IoT device has been compromised by an attacker while the RRC connection of this IoT device has been suspended.
2. The IoT device Resume RRC connection with RRCResumeRequest to gNB.
3. gNB responds with RRCReject with a wait timer.
4. Instead of IoT device go back to INACTIVE as expected, the IoT device continues to send RRCResumeRequest to gNB using the same I-RNTI.

* For the RRC re-establishment procedure, the attack is similar to RRC Resume with small differences like the following:

1. The same as in RRC Resume, it is assumed that an IoT device has been compromised by an attacker or misbehaving.
2. After this IoT device established connection with 3GPP network, network may notify the IoT device to perform some action (e.g., Reconfigure connection according to notification).
3. Instead, this IoT device ignore the network notification intentionally and trigger RRC re-establishment. After RRC re-establishment are successful, network notifies the IoT device to perform the same action again, and the IoT device triggers RRC re-establishment again. Repeat Step2 to Step3.

After the UE get in RRC-CONNECTED state, it can send RRC messages on SRB1 or NAS messages carried over SRB2.

If an attacker is able to compromise a group of IoT devices to do the exact same behaviour, this may result into a serious DoS attacks that can exhaust the gNB RRC resources and drive the gNB into overload and possibly becomes unavailable.

### 6.7.2 Solution details

This solution enables gNB to detect RRC resume/RRC re-establishment, RRC messages sent on SRB1, NAS messages carried over SRB2 DoS attack and allow the gNB to dynamically inform 5GC for further actions.

Per-gNB and per-UE counters will potentially be standardized by 3GPP but their threshold values are left for implementation.

The details are shown in the following figure using RRC resume/RRC re-establishment as an example.



Figure 6.7.2.1-1 Procedure for protecting gNB from RRC resume and RRC Re-establishment DoS attack

1. Configure the gNB with a per-gNB threshold (Threshold1) for the number of receiving RRCResumeRequest/RRCReestablishmentRequest messages within a specific period of time at the gNB.
2. Configure the gNB with a per-UE threshold (Threshold2) for the number of received RRCResumeRequest/RRC Reestablishment for the same UE identity, i.e., I-RNTI/C-RNTI.
3. UE sends RRCResumeRequest/RRCReestablishmentRequest to gNB.
4. gNB verify resumeMAC-I/shortMAC-I. If verify fail, gNB sent RRCReject or fallback to RRCSetup; if verify success, perform following steps.
5. gNB counts the number of total RRCResumeRequest/RRCReestablishmentRequest messages received at the gNB within a period of time, If the number exceeds Threshold1, the gNB starts tracking the received messages per UE using the UE temporary identifier(I-RNTI/C-RNTI).
6. gNB further counts the number of of received RRCResumeRequest/RRCReestablishmentRequest messages for a specific I-RNTI/C-RNTI after the threshold1 is exceeded in step 5, if the number also exceeds Threshold2, the gNB flag this UE as an attacking or misbehaving UE.
7. gNB reports the attacking UE(s) information using the SecurityAlarmNotification message. gNB includes the list of attacking UE(s) temporary identities (RAN UE NGAP ID/AMF UE NGAP ID as defined in TS 23.501) in the SecurityAlarmNortification message sent to 5GC for further action.

NOTE: SecurityAlarmNotification message include some essential parameters that are needed to identify the attacking UEs, e.g., RAN UE NGAP ID and AMF UE NGAP ID as defined in TS23.501[10]. Some other parameters as Number of received RRCResumeRequest/ RRCReestablishmentRequest in a period of time can also be included.

1. 5GC, e.g., AMF/SEAF, should map the temporary indentity of AMF UE NGAP ID to longer lifecycle identity (e.g TMSI) and should be able to enforce the selected action on the UE while accessing the current gNB or if the UE tries to access the network over other gNBs under the control of the specific AMF/SEAF.
2. gNB rejects RRCResume with a timer (waittimer) or fallback to RRCSetup to against the attacking UE.

The main purpose for Threshod1 is to avoid having the gNB to start tracking all UEs unnecessarily. This also possible by allowing the gNB to track all UEs behaviour for a short period of time. In other words, if gNB does not receive an additional RRCResumeRequest for UE1 for a specific period of time, gNB can stop tracking such UE.

For RRC messages sent on SRB1 and NAS messages carried over SRB2, C-RNTI is used to identify the same UE.

### 6.7.3 Evaluation

This solution address key issue #5 and has the following benefits:

- Enable gNB to identify UEs which cause DoS attack using RRC resume/RRC re-establishment, RRC messages sent on SRB1, and NAS messages carried over SRB2.

- Set two thresholds (per-gNB threshold and per-UE threshold) to avoid the gNB to track all UE at the beginning, this mechanism can enable gNB save processing resource as much as possible during detecting DoS attack.

- Reject specific UE (IoT device) which launches attack without affecting normal service of other IoT devices.

- gNB informs 5GC to enable 5GC take further preventive actions against the specific UE directly even in the case the UE move to other gNB.

## 6.8 Solution #8: Security solution for protection of interface used by NIDD procedures

### 6.8.1 Introduction

This security solution is related to the key issue #9: Protection of NIDD interfaces, concerning protection of the interface utilized by the NIDD procedures.

Non-IP Data Delivery (NIDD) is a part of CIoT EPS optimisations and can be used to deliver unstructured data. NIDD is further defined in TS 23.401 [5] clause 4.3.17.8.1 and in TS 23.682 [6] clause 4.5.14. EPS can deliver the Non-IP data using the Service Capability Exposure Function (SCEF) node which is replaced by the Network Exposure Function (NEF) node in 5GS.

The interface utilized by the NIDD procedures between the NEF and the Application Function (AF) is supposed to transfer data and therefore needs to be properly secured by providing confidentiality, integrity and replay protection.

### 6.8.2 Solution details

This solution proposes to reuse the security solution based on TLS defined in clause 12 in TS 33.501 [8].

### 6.8.3 Evaluation

The proposed solution fulfils the potential security requirements given in the related key issue.

## 6.9 Solution #9: Security protection of small data at idle mobility

### 6.9.1 Introduction

This solution addresses key issue #2: Integrity protection of small data and key issue #3: Encryption of small data in this TR.

### 6.9.2 Solution details

This solution is an enhancement of solution #1 to address the issue of transferring the user data during a Registration procedure that may result in a change of AMF. A potential issue of sending small data in the Registration Request is that AMF change may involve a horizontal KAMF derivation, thereby the target AMF not being able to process the small data included in the Registration Request message.

In case of AMF change, the target AMF forwards the Registration Request message to the source AMF and the source AMF checks the integrity of the Registration Request. In addition, the source AMF decrypts the encrypted data IE and sends the decrypted data back to the target AMF.



The procedure proceeds as follows.

1. UE sends a Registration Request that contains the small data. The small data is encrypted using the initial NAS protection mechanism in TS 33.501 [8].
2. The new AMF forwards the Registration Request to the old AMF identified by the 5G-GUTI in the Registration Request. The new AMF may be same as the old AMF.
3. The old AMF verifies the integrity of the Registration Request and if the verification is successful, decrypts the small data.
4. The old AMF sends the UE context and the decrypted small data to the new AMF. The small data to be forwarded is now available at the new AMF.
5. (optional) If the new AMF received a new KAMF derivation indication, the new AMF performs the NAS SMC procedure to activate the new security context based on the new KAMF.
6. The new AMF sends a Registration Accept message to the UE.

The rest of the procedure is same as in TS 23.502 [15].

### 6.9.3 Evaluation

* Based on the initial NAS security protection, the small data included in the Registration Request message is ciphered and integrity protected. Therefore, the key issue #2 and key issue #3 are satisfied by this solution.
* The impact of the solution is that the source AMF needs to supply the decrypted small data to the target AMF.
* Sending small data in 5GS NAS messages is a new feature. A non-security outstanding issue of this feature is whether the UE can include small data in Registration Request messages. This solution is only useful if for architectural/efficiency reasons, it is decided to include small data in Registration Request messages.

## 6.10 Solution #10: Security solution for small data at idle mobility using the Registration Complete message

### 6.10.1 Introduction

This solution addresses key issue #2: Integrity protection of small data and key issue #3: Encryption of small data in this TR.

### 6.10.2 Solution details

This solution is an enhancement of solution #1 to address the issue of transferring the user data during a Registration procedure that may result in a change of AMF. The issues with these Registrations procedures is that the new AMF may not be able to decrypt the user data as it may not either get the used security context from the old AMF (e.g. KAMF change) or support the algorithm choice of the old AMF.

To avoid this issue the UE does not send the user data in the Registration Request when there is a risk of AMF change during to the possibility of idle mobility but sends the user data in the Registration Complete instead. In these cases, there will be a Registration Complete message due to the need to allocate a new GUTI and therefore this solution will not increase the number of messages sent between UE and AMF. The Registration Complete message is always integrity protected and ciphered. Using the Registration Complete to transfer the data means that the new AMF will be able to decrypt and hence successfully receive the data without the need for additional security procedures. It also avoids the need to send the data twice if the Registration Request is repeated in the NAS Security Mode Complete message due to the initial NAS security procedure.



Figure 6.5.10-1: Small data protection at idle mobility

The procedure proceeds as follows:

1. UE sends the Registration Request that may result in a change of AMF

2. New AMF fetches the MM context form the old AMF

3. New AMF optionally authenticates the UE and trigger the NAS Security Mode Command procedure as needed.

4. New AMF sends the Registration Response with a new GUTI.

5. UE sends the Registration Complete containing the user data.

### 6.10.3 Evaluation

As the Registration Complete message is always ciphered and integrity protected, then the UP data is ciphered and integrity protected. Hence, the requirements for key issue #2 and key issue #3 are satisfied by this solution.

The impact of the solution is that the UE and AMF need to support having the UP data in the Registration Complete message.

Sending small data in 5GS NAS messages is a new feature. A non-security outstanding issue of this feature is whether the UE can include small data in registration procedures. This solution is only useful if for architectural/efficiency reasons, it is decided to include small data in registration procedures.

## 6.11 Solution #11: Security-Property-Group-based Mitigation for DDoS Attack Triggered by Malicious Applications on the UE

### 6.11.1 Introduction

This solution addresses key issue #4. DDoS attack triggered by malicious applications on the UE may lead to signalling overload on the CN.

In real world, an attacker may compromise a lot of IoT devices to trigger a DDoS attack, e.g. in 2016, 3 teenagers created Mirai which exploited a default weak password vulnerability to infect IoT devices. Mirai searched and compromised thousands of IoT devices who have the same vulnerability. Finally, they triggered a DDoS attack to a root DNS server after control one hundred thousand IoT devices, and shut it down for several hours, which cause large-scale disconnection on East Coast of the US.

In 5G, the number of IoT devices grows explosively, the situation will be even worse. The attacker may control larger number of IoT devices with a rapidly spreading worm (e.g. Mirai and its varietals). When the huge number of the IoT devices are commanded to trigger DDoS attack to the same AF together, it may be also a DDoS attack to the operator network, e.g. massive IoT devices send the NAS signalling with small data to the same AMF together, or massive IoT devices send the UP data to the same UPF/NEF together, etc., which causes signalling overload.

Currently, when the NEs are overload, the NEs may reject the UEs with low priority in order to avoid crash, but it is a DoS attack to some of the UEs in a sense. However, if the NEs does not do this, all of the UEs controlled by this NE may be DoS too.

The solution proposes a Security-Property-Group assignment mechanism to classify IoT devices who may be compromised by the same attacker. The solution also proposes a DDoS mitigation mechanism. The network assigns Security-Property-Group ID for each UE, detects the potential DDoS attack based on Security-Property-Group, and mitigates the DDoS attack towards the CN within Security-Property-Group. The solution will be more precise than current signalling overload solution.

### 6.11.2 Solution details

#### 6.11.2.1 Security-Property-Group assignment mechanism

##### 6.11.2.1.1 Principle of assignment

The attacker often exploits the same vulnerability to compromise a large of IoT devices. For Mirai, the compromised IoT devices have the same default weak username and password, because these compromised IoT devices have the same properties, e.g. the same application, operate system, hardware, Default Configuration, etc. If network finds a way to classify these properties into a group, the network may mitigate DDoS attack based on this group. We call it as Security-Property-Group. It will be more accurate and efficient to control the misbehaving IoT devices compromised by the same malicious applications.

In 3GPP, there are many IEs which are related to the properties above. An example for related 3GPP IEs is listed in table 6.11.2.1.1-1.

**Table 6.11.2.1.1-1 an example Related 3GPP IEs for Security-Property-Group**

|  |  |
| --- | --- |
| **Properties** | **Related 3GPP IEs** |
| Application | Application Identity, e.g. Internal-Group Identifier, application ID, etc. |
| OS | ME Identity, e.g. SV in IMESV |
| Hardware | ME Identity, e.g. TAC in IMEI |
| Default Configuration | ME Identity, e.g. TAC in IMEI |

The network may collect the 3GPP IEs above, classify the IoT devices by assigning Security-Property-Group ID derived according to those 3GPP IEs. This ID should be stored in the UE context in CN NEs, e.g. AMF, SMF, UPF, etc. The network may mitigate DDoS attack within the Security-Property-Group.

##### 6.11.2.1.2 Assignment Procedure



**Figure 6.11.2.1.2-1 Security-Property-Group Assignment Procedure**

1. UE sends Registration Request message to the AMF.
2. The AMF retrieve security group related IEs, e.g. gets UE’s IMESV in NAS SMC, gets Internal-Group Identifier from UDM, etc.
3. The AMF assigns a Security-Property-Group ID according to the IEs described above. The UEs who have the same IEs will be assigned to the same Security-Property-Group ID.
4. The AMF sends the Security-Property-Group ID to other NEs, e.g. SMF, UPF, etc.
5. These NE stores the Security-Property-Group ID in the UE context.

#### 6.11.2.2 DDoS attack mitigation

##### 6.11.2.2.1 DDoS attack on AMF/SMF

When an attacker triggers DDoS attack to an AF by malicious application on the UEs, for infrequent small data transferring, the massive UEs may wake up together, and send the UP data in the NAS signalling to the same AMF/SMF at the same time, which may lead to signalling overload on the AMF/SMF.

The AMF/SMF extracts UE ID (e.g. 5G-GUTI) from the NAS request message when receiving the NAS message, finds the Security-Property-Group ID in the UE context and counts for the Security-Property-Group ID. If AMF/SMF is overload, the AMF/SMF may reject the NAS request of UEs in the specific Security-Property-Group who behaves abnormally until the AMF/SMF is recovered, e.g. the counter for the specific Security-Property-Group ID far in excess of the daily average.

##### 6.11.2.2.2 DDoS attack on UPF/NEF

When an attacker triggers DDoS attack to an AF by malicious application on the UEs, the massive UEs may wake up together, and send the UP data to the same UPF/NEF at the same time, which may lead to signalling overload on the UPF/NEF.

The UPF/NEF extracts UE ID (e.g. source IP or source MAC) from the NAS request message, finds the Security-Property-Group ID in the UE context and counts for the Security-Property-Group ID. If UPF/NEF is overload, the UPF/NEF may adjust a low QoS for the UEs in the specific Security-Property-Group who behaves abnormally.

### 6.11.3 Evaluation

TBD

Editor’s Note: Whether or not the solution needs standardization is FFS.

Editor’s Note: Whether the solution introduces new DoS attack is FFS.

Editor’s Note: The impact on UPF signalling is FFS.

## 6.12 Solution #12: Security Solution on DDoS attack mitigation

### 6.12.1 Introduction

This solution addresses key issue #4 Signalling overload due to Malicious Applications on the UE. If a large number of misbehaving UEs send user plane packets to the network may lead to DDoS attack against CN, e.g. UPF. The key issue proposes to detect the attack and protect the network against DDoS attack.

This solution assumes that the UE is a dual-mode UE (e.g. able to receive and send).

The key issue assumes that the malicious behaviour on the UE is the result of an attacker having access to the application on the UE which it can instruct to make certain requests to the network. An attacker could have obtained this access through the over the top service and could for example instruct the UE to set up dedicated bearers or request access to certain network slices. An important assumption of this key issue is that the UE part that is responsible for executing the radio instructions remains untouched.

The 5GC need to control the traffic between UE and network if DDoS attack happens. So this solution is proposed to dynamically enable the network to instruct the UE to discard the type of traffic that matches the DDoS packet of user plane and maintain the traffic of the normal connections. The action of discarding malicious packet is done in UE side.

### 6.12.2 Solution details

#### 6.12.2.1 Architecture

The proposed solution focuses on discarding the DDoS packet in UE side based on the instruction form network side. The network side of the solution assumes that the detection capability, security decision making capability and their logic are already in place and exist. The detection function (DF) collects the UE and network activities to detect abnormal UEs and their behaviour (e.g. potentially substantial increase of traffic compared to known trends or usage of the IoT device). For example, the DF can be NWDAF as defined in TS 23.501 [10]. The conclusion for normative work based on Solution 8 in TR 23.791 [11] is proposed to use NWDAF to identify the misused or hijacked mIoT terminals. Based on the received report from DF, security function (SF) (can be co-located with DF or PCF) makes decisions to mitigate against the attack by instructing the PCF to create packet filter and deliver it to UE. If UE’s packet matches rules defined in the filter, the packet is regarded as malicious packet and discarded at the UE side.

#### 6.12.2.2 Procedure

The UE’s dynamic packet filtering delivery method to mitigate DDoS attack is depicted in figure 6.12.2.1-1.



Figure 6.12.2.1-1: UE’s packet filtering method to mitigate DDoS attack

1. The SF request the detection report to DF;
2. DF reply the detection report to SF;
3. Based on the report, the SF make decisions and create instructions;
4. SF send the instructions to PCF. The instructions contain the UE\_ID, exception ID, exception level, exception trend as described in TS 23.288 [12], which indicates analysis result based on detection. For example, SF instructs to block the data transmissions between UE and target IP if the DoS attack is detected. Based on the detection result, which may indicate the attack is gone after a period of time, the SF send new instructions to PCF to allow the data transmissions;
5. The PCF create packet filters based on received instruction and/or local policy. The filters include IP address, source port, target port and so on as described in clause 5.7.6 in TS 23.501 [10];

6-8. The PCF sends packet filter(s) and indicator to UE, which indicates that these packet filters are used for discarding the packets. This indicator can be a specific 5QI;

9. UE receives and stores packet filters and indicator. If the uplink data matches with the packet filters, the UE discard the packets.

### 6.12.3 Evaluation

The proposed solution fulfils the potential security requirements of key issue#4. When used, the solution makes it possible to mitigate DDoS attack originated from UE side. The solution will not disconnect the UE from the network, but only allows the UE to discard malicious packets. This solution has a flow-based granularity because only packets in flows that are causing the DDoS on the network are discarded in the UE while other packet flows are not be effected RAN and network elements will benefit since the packets that are causing DDoS are discarded in UE without having to be processed in the network. CN will significantly realize resource saving when DDoS attacks are prevented.

Detection and creating packet filters are performed on the network side. The DF and SF can be the NWDAF as defined in TS 23.501[10]. SF sends and updates instructions to PCF based on detection results. This solution requires that the PCF to take instruction from SF into consideration when making a packet filter. This solution also requires that the UE supports discarding the packet based on the indicator and filter rules.

## 6.13 Solution #13: Security solution for small data using key refreshing

### 6.13.1 Introduction

This security solution is related to the solution for Key Issue #7: Key refreshing for protection of small data and covers infrequent and frequent small data.

### 6.13.2 Solution details

#### 6.13.2.1 Support for infrequent small data transmission

For infrequent small data, only solutions for small data transport within NAS are considered. Based on operator policy the AMF may use a counter or a timer for NAS key refreshing. The AMF detects based on the CN parameters that the UE has an infrequent small data traffic pattern and initializes the counter at the initial registration. The AMF shall increment the counter for each small data NAS PDU and if the threshold is reached, the AMF shall initiate NAS key refresh procedure (TS 33.501 [8], clause 6.9.4.3).

#### 6.13.2.2 Frequent small data communication

Frequent small data is transferred over the user plane in all solutions and the UE returns in RRC-INACTIVE/RRC-SUSPEND (depending on the solution) after small data transmission. The RAN keys are refreshed after each transition to RRC-CONNECTED mode. Stationary UEs may have always the same PCI and ARFCN-DL/EARFCN-DL, thus for key derivation at state transition only the NH and NCC value can be varied. For this reason, the RAN shall start a counter for INACTIVE/SUSPEND transitions and once the counter exceeds the limit based on operator policy, the RAN shall initiate a complete new key refresh, e.g. the RAN shall send an <RRC Connection Setup> message on SRB0 to the UE in order to proceed with RRC connection establishment as if the UE was in RRC\_IDLE.

### 6.13.3 Evaluation

The proposed solution fulfils the potential security requirements given in the related key issue #7.

## 6.14 Solution #14: Privacy protection of new parameters for CIoT included in NAS messages

### 6.14.1 Introduction

This solution addresses key issue #12: Privacy protection of new parameters for CIoT included in NAS messages.

TR 23.724 [2] recommends many solutions for normative work, where some solutions requires that new parameters for CIoT need to be included by the UE in the NAS messages to the AMF. Some of these new parameters for CIoT may require encryption if they are privacy sensitive.

Each new parameter for CIoT introduced by the recommended solutions in TR 23.724 [2] for CIoT Rel-16 needs to be checked whether they are privacy sensitive or not i.e. whether they can be sent in clear text or whether they need to be sent ciphered.

### 6.14.2 Solution details

The protection of the initial NAS message in 5G was defined in Rel-15 and is described in clause 6.4.6 in TS 33.501 [8].

It is proposed to re-use the security solution for the initial NAS message in Rel-15 described in clause 6.4.6 in TS 33.501 [8] in order to provide privacy for the new parameters for CIoT which are privacy sensitive.

### 6.14.3 Evaluation

TBD

## 6.15 Solution #15: Efficient integrity protection for small data transmissions with immediate result

### 6.15.1 Introduction

This solution addresses the key issue #1 "Efficient frequent small data transmissions" and the key issue #2 "Integrity protection of small data". This solution reduces the overhead of MAC-I (Message Authentication Code-Integrity) included in the small data when integrity protection is applied in the UP. The relative overhead of MAC-I is high as the payload size is small, and thus it decreases the effective user data throughput. The proposed solution decreases the overhead of transmitting one MAC-I from 4 octets to 1.

### 6.15.2 Solution details

#### 6.15.2.1 General

The MAC-I for a message marked as 'first message' is computed in the traditional way.

The MAC-I for a next message between the same two entities uses the bits to be integrity protected from that next message as input for the MAC computation, prepended with

- the bits to be integrity protected from the three previous messages if none of these has been marked as a 'first message', or

- the bits to be integrity protected from the previous messages up to and including the last message marked as 'first message' if the last message marked as a 'first message' is at most the third previously sent message.

Figure 6.15.2-2 illustrates this solution.

The MAC-I is truncated to 8 bits when one of the reserved bits in the PDCP header, the 'T' bit, equals 1. The full 32-bit I-MAC is used when the 'T' bit equals 0 for backwards compatibility.

In order to indicate whether the transmitted data is the 'first message' or not, one of the reserved bits in PDCP header is used, the 'N' bit. The value of 0 is set when the message is a 'first message', and the value of 1 is set when the message is a 'next message' i.e. not a 'first message'. The transmitter and receiver store the last three messages for use in the (truncated) MAC-I computation.

The 'T' and 'N' bit combinations of (1,0) and (1,1) yield a 3\*8 bit saving in MAC-I length.

A 'T' and 'N' bit combination of (0,0) means use full 32-bit I-MAC and do not use previous messages for the I-MAC, which means that this solution is backwards compatible.

A series of messages with a 'T' and 'N' bit combination of (1,1) can be ended with a message with a T' and 'N' bit combination of (0,1), so the last three messages of the (1,1) series obtain the full 32-bit I-MAC protection. This is useful when the transmitter wants to switch over to the legacy integrity protection using the combination (0,0).

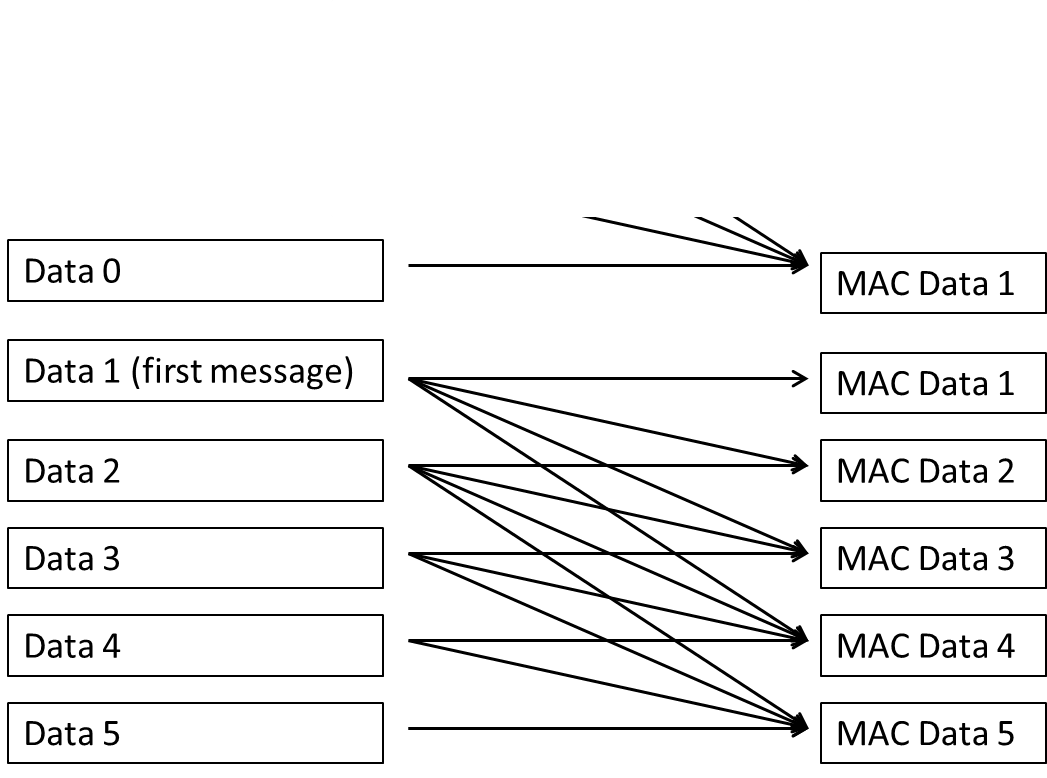


Figure 6.15.2-1 Efficient integrity protection for small data transmission

#### 6.15.2.3 Receiver behaviour

A receiver sets the integrity status of a received message marked as a 'first message' using a truncated MAC-I, to 'NOT OK' when any of the three previously received messages were marked as a 'first message' using a truncated MAC-I. This is to defeat an attacker that marks many or all messages with a truncated MAC-I as a 'first message'', so causes their effective integrity protection to be less than 4\*8 bits.

The receiver sets the integrity status of all other received message initially to 'OK' before it checks the integrity of these messages.

Then, the receiver compares the received (truncated) MAC-I with the computed (truncated) MAC-I over the received data. If the received and computed (truncated) MAC-Is are different, the integrity status of all received messages that have been used to compute the (truncated) MAC-I is set to 'NOT OK'. E.g. if the computed MAC Data 2 in Figure 6.15.2-1 is different from the received one, the receiver sets the integrity status of Data 1 and Data 2 to 'NOT OK'.

The receiver forwards a message to its destination if that message is no longer needed for (truncated) MAC-I computation and its integrity status is 'OK'. The receiver deletes a message if that message is no longer needed for (truncated) MAC-I computation and its integrity status is 'NOT OK'. E.g. the receiver forwards message 1 in Figure 6.15.2-1 to its destination when message 4 has been received and MAC DATA 1, 2, 3 and 4 have all been found correct.

### 6.15.3 Evaluation

This solution reduces the overhead caused by the MAC-I from 4 octets to 1 octet in a similar, but different manner than solution #2.

The advantage of this solution is that the integrity protection of each received message can be checked immediately after reception. This means that, in contrast with solution #2, this solution provides defence against a DOS attack, since the integrity status of fake messages using a truncated MAC-I from a DOS attacker have a probability of only 1 in 256 of *not* being marked as 'NOT OK' by the receiver immediately after reception. This is not the case for the first three messages of the solution #2. An attacker could send up to three messages from each fake address for flooding the network when solution #2 is deployed.

The integrity protection 'strength' is limited for the lastly received message using a truncated MAC-I, namely, assuming that all bits of the MAC-I resist existential forgery against chosen plaintexts, there is a probability of 1 in 256 that the current message is fake but has a correct truncated MAC-I. However, this is much better than no protection at all. The probability of not detecting that message as a forged message drops by a factor of 256 with every newly received message using a truncated MAC-I down to eventually 1 in 2564, which is the same as when the full 4-octet MAC-I would have been used.

Furthermore, suppose an attacker forges one single transmission with a truncated MAC-I, that is, one single message and the first MAC-I to which it contributes. Even if the attacker could successfully forge the first truncated MAC-I involving this single message, he just has to hope the three subsequent MAC-Is involving this single message are correct, as he does not yet know what the three subsequent messages will be.

Note: The presence of COUNT in messages prevents replay attacks.

For every received message, the receiver needs to compute the (truncated) MAC-I over the received message and zero to three previously received messages.

The PDCP PDU header is integrity protected by the (truncated) MAC-I. If an attacker has been able to change the 'T' bit and/or the 'N' bit, which are the bits in the PDCP header that have been introduced by this solution, this will cause one or more (truncated) MAC-I failures and can therefore be detected by the receiver.

The data sequence number SN together with the HFN make up the value of COUNT. As the COUNT value is integrity protected by truncated MAC-Is and/or a MAC-I, manipulation of the SN by an attacker is detected in the same way and with the same probabilities as manipulation of the message content.

This solution addresses key issues #1 and #2.

## 6.16 Solution #16: Solution to Identify Misbehaving UEs

### 6.16.1 Introduction

This solution addresses the key issue #4 "Signalling overload due to Malicious Applications on the UE ". This solution provides mechanism to identify misbehaving UEs.

### 6.16.2 Solution details

The solution is described in clause 6.9 in TS 23.288 [12] to identify misbehaving UEs.

The NWDAF collects UE behavioural information for data analytics from 5GC NFs, such as Communication start or end time, UL or DL Packet Latency, UL or DL data rate, etc. The NWDAF detects the UEs with abnormal behaviour, including serious misbehaviours that are considered DDoS attack by using analysis or other tools. The NWDAF identifies these misbehaving UEs and then notifies AMF, or SMF, or PCF to take actions for the identified specific UE or specific UE group based on operator policy.

Editor’s Note: Privacy issues with collecting UE data is FFS.

### 6.16.3 Evaluation

TBA

## 6.17 Solution #17: Solution to Mitigate DDoS Attack based on RAN caused by Massive Number of Misbehaving CIoT UEs

### 6.17.1 Introduction

This solution addresses the key issue #4 “Signalling overload due to Malicious Applications on the UE”. The RAN is able to protect itself against overload case caused by massive number of misbehaving CIoT UEs.

The solution assumes that the attacker controls massive infrequent CIoT UEs who send the user data in NAS signalling by having access to the application on the UE, and the UE part that is responsible for executing the radio instructions remains untouched. When the misbehaving CIoT UEs controlled by the attacker trigger a DDoS attack to the external AF, the RAN is a potential victim due to the need to pass heavy NAS traffic flow across the RAN given there are sufficiently large number of misbehaving UEs served by the same RAN. The RAN has high risk of overload due to highly faster data transmission rate than 4G.

This solution provides mechanism for RAN to reject the malicious CIoT UEs in case of overload. Detection function (DF) detects potential malicious i CIoT UEs and reports the UE list to the AMF, the AMF distributes part of the UE list to the affected RAN.

RAN will handle the list based on RAN status, when the RAN works well, it does not handle the potential malicious UEs, because DF may not detect the UEs with 100% precision. Only in case that RAN is going to be overloaded, it may handle these potential malicious UEs with high priority so that the RAN has more resource for normal UEs. When the RAN recovers, the mitigation will be stopped. It is a balance between UE and RAN usability, and it is a way to reduce impact of UE’s normal service.

### 6.17.2 Solution details

#### 6.17.2.1 Architecture

The solution is used to mitigate potential DDoS attack on the RAN caused by a huge number of misbehaving CIoT UEs.

The detection function (DF) could detect misbehaving UEs and outputs their misbehaviours (e.g. DDoS attack) to AMF. The DF can be NWDAF, and could identify malicious UEs as defined in TS 23.288 [12]. Based on the received report from DF, AMF makes decisions whether to control the UEs in the RAN. For example, if there are plenty of misbehaving UEs in the same RAN who are controlled to attack an external AF, it may be also a potential DDoS attack to the RAN, the AMF may set a blacklist on the RAN to reject the malicious CIoT UEs in overload case.

#### 6.17.2.2 Procedure

The RAN-based mechanism to mitigate DDoS attack is depicted in figure 6.17.2.2-1.



Figure 6.17.2.2-1: RAN-based Mechanism to Mitigate DDoS Attack

1. CIoT UE was received a 5G-GUTI when the UE registered to the network. When the misbehaving UEs are attacking an AF, the UEs are in CONNECTED and continuously send the NAS messages, and RAN will maintain some UE context for i CIoT UEs.
2. The DF may detect DDoS attack, e.g. as mentioned in solution 16.
3. DF sends the detection report to AMF, which includes misbehaving UE IDs.
4. If large number of the malicious UEs are in the same RAN) (exceed a specific threshold), the AMF shall get the RAN UE NGAP IDs from UE contexts and construct a list, then notify the list to the specific RAN node).
5. The AMF sends the list to the RAN.
6. The RAN stores the RAN UE NGAP ID list in blacklist. There are two options to remove the UE from blacklist. Option 1: The RAN may setup a timer for the blacklist. When the timer is expired, the UEs are removed from the blacklist. However, when the RAN is continuously overloaded or new RAN UE NGAP ID is added, the timer may be reset to the start value after wrapping around to extend the validity of the blacklist for another timer cycle. Option 2: Based on the detection result, which may indicate the attack disappears after a period of time, the DF may send normal UE IDs to the AMF, and the AMF may notify the RAN to remove the normal UEs from the blacklist.
7. When the RAN experiences to be overloaded, the RAN performs the mitigation procedures as described from step 7 to step 10. However, when the RAN is still operating normally, e.g. isolated DoS attack does not impact RAN performance, previous mitigation eased overloading, etc., the mitigation procedure shall not be performed.

NOTE 1: This mechanism is to protect the RAN from being overloaded caused by massive CIoT UEs. It is assumed that the misbehaving UEs will not move together, moved UEs will not significantly affect the other RAN. Thus, the blacklist is not needed to be shared with other RAN.

1. For infrequent CIoT UEs, the RAN may release the RRC connection identified by the stored blacklist if the UE is in CONNECTED.

For frequent CIoT UEs, the RAN may suspend the RRC connection identified by the stored blacklist if the UE is in CONNECTED, and assign a new ResumeID for the UE.

1. The UE who is commanded to trigger a DDoS attack may re-connect to the RAN immediately.

For infrequent CIoT UEs, the UE sends RRC Early Data Request with S-TMSI to the RAN.

For frequent CIoT UE, the UE sends RRC Resume Setup with ResumeID to the RAN.

1. The RAN in overload case, compares S-TMSI or ResumeID with the blacklist, if the UE indicated by S-TMSI/ResumeID is in the blacklist, the RAN shall reject the UE with a wait timer, and the wait timer may be max value as specified in TS 38.331 [13].
2. The RAN sends RRC Reject message to the UE with the wait timer, and the UE shall not connect to the RAN again during the wait timer period. The misbehaving UE will be rejected by the RAN, and the RAN will not waste resources to establish a UE context for the misbehaving UE.

### 6.17.3 Evaluation

The solution fulfils the potential security requirements of KI#4. The 5G network entity, RAN could be able to protect itself from signalling overload.

When the RAN is overloaded, the RAN may control the misbehaving UEs received from DF, which means the RAN protects itself from signalling overload. The benefits and drawbacks are as follows:

**Benefits:**

1. Guarantee RAN usability: RAN can protect itself without any UE change from draining resource caused by massive malicious CIoT UEs without any UE change.
2. Guarantee UE usability: DF cannot guarantee 100% precision, and the misinformation exists. In order to mitigate UE impact caused by the misinformation, the RAN will not launch the blacklist to isolate the UEs if the RAN is not overloaded. The solution will mitigate unnecessary complaint caused by misinformation.

**Drawbacks:**

The RAN will not control the misbehaving UEs immediately, instead, if the RAN could tolerate the attack, the mitigation will not be triggered, and the malicious data flow will congest on the NEs behind. Thus, AMF, may not be protected.

Maintaining the blacklist introduces some overhead.

## 6.18 Solution #18: Security solution for UL small data transfer in RRC Suspend and Resume with early data transmission (EDT)

### 6.18.1 Introduction

This solution addresses key issue #3: Encryption of small data and key issue #8: Key and mac size for protection of small data in this TR.

This security solution address solution 19: 5GS UP Optimization for Infrequent Small Data Transmission in SA2 TR 23.724 [2]. This solution is to optimize small data transmission for the UEs from CM-IDLE mode. It enables transfer of user plane data without need for the Service Request procedure. According to solution 19 in SA2 TR 23.724 [2], it is proposed to keep AS context in the NG-RAN including information the UPF connection and relevant QoS flow(s) to be used for the connection, even when UE moves into CM-IDLE. When UE resumes the connection, the NG-RAN uses the information to activate DRB, AS security and User Plane connectivity over N3 for the small data packet delivery to the UPF.

In EPS/LTE Rel-15, early data transmission (EDT) feature was added to the RRC Connection Resume/Suspend procedures in eNB as specified in TS 33.401 [7]. Uplink user plane data is included as early data transmission with the RRC Connection Resume Request (msg 3). In the EPS/LTE Rel-15, RRC Connection Resume Request (msg 3) only supports encryption of uplink user plane data (EDT). As described in T S 33.401 [7], the UE and the target eNB uses the newly derived KUPenc for ciphering/deciphering of the UL EDT data in PDCP layer in the RRC Connection Resume Request message, and user DL data (if included) in PDCP layer in the RRC Connection Suspend or RRC Connection Resume message.

This solution proposes to re-use the security solution for RRC Suspend and Resume procedures with EDT as defined in EPS/LTE Rel-15 in clause 7.2.11 in TS 33.401 [7] for E-UTRA connected to 5GC.

### 6.18.2 Solution details

#### 6.18.2.1 UL data transmission from CM-IDLE with Early Data Transmission

The following figure shows a single MO small data delivered from the UE using Early Data Transmission.



**Figure 6.18.2.2-1: Single MO data Transmission using 5GS UP Optimization and Early Data Transmission (EDT)**

Figure 6.18.2.2-1 shows the following steps:

1a. The UE sends RRC Connection Resume Request with the UL small data included as UL EDT (Early Data Transmission) with the RRC Connection Resume Request (msg 3) on SRB0 and hence it is not integrity protected. The UE includes information to be used for context identification and re-establishment in the RRC Connection Resume Request message: The Resume ID and a ShortResumeEDTMAC-I.

For protection of the UL EDT in the RRC Connection Resume Request message the description in clause TS 33.401 [7] for protection of EDT is re-used.

1b. The RAN immediately suspends the RRC connection (to minimize UE power consumption) as described in TS 23.724 [2].

2. The RAN forwards the UL data received from the UE to the UPF as described in TS 23.724 [2].

3. UE and RAN remain suspended as described in TS 23.724 [2].

#### 6.18.2.2 Connection Suspend procedure using the Early Data Transmission (EDT) feature

This procedure is used by the RAN to suspend the connection if 5GS UP Optimization is supported as described in solution 19 in TS 23.724 [2].

It is expected that the security solution defined in clause 7.2.11 in TS 33.401 [7] for EDT is re-used for this scenario.

### 6.18.3 Evaluation

The proposed security solution fulfils the potential security requirements of KI#3: Encryption of small data.

## 6.19 Solution #19: Solution to Mitigate DDoS Attack on AMF caused by Massive Number of Misbehaving CIoT UEs

### 6.19.1 Introduction

This solution addresses the key issue #4 “Signalling overload due to Malicious Applications on the UE”. The AMF is able to protect itself against signalling overload caused by massive misbehaving CIoT UEs.

The solution assumes that the attacker controls massive CIoT UEs who send the user data in NAS signalling by having access to the application on the UE. When the misbehaving CIoT UEs controlled by the attacker trigger a DDoS attack to the external AF, the AMF are potential victims due to heavy NAS signalling to the AMF given there are sufficiently large number of misbehaving UEs served by the same AMF. The AMF has high risk of overload due to highly faster data transmission rate in NAS signalling than 4G.

This solution provides mechanism for AMF to release PDU session of the malicious CIoT UEs in overload case. Detection function (DF) detects potential malicious CIoT UEs and reports the UE list to the AMF, and the AMF stores the list.

AMF will handle the list based on AMF status, when the AMF works well, it does not handle the potential malicious UEs, because DF may not detect the UEs with 100% precision. Only in case that AMF is going to be overloaded, it may handle these potential malicious UEs with high priority so that the AMF have more resource for normal UEs. It is a balance between UE and AMF usability, and it is a way to reduce impact of UE’s normal service.

### 6.19.2 Solution details

#### 6.19.2.1 Architecture

The solution is used to mitigate potential DDoS attack on the AMF caused by a huge number of misbehaving CIoT UEs.

The detection function (DF) could detect misbehaving UEs and outputs their misbehaviours (e.g. DDoS attack) to AMF. The DF can be NWDAF, and could output malicious UEs as defined in TS 23.288 [12]. The AMF could set a blacklist, and mitigate the potential DDoS attack by releasing the PDU sessions of malicious UEs in the blacklist in overload case.

#### 6.19.2.2 Procedure

The AMF-based mechanism to mitigate DDoS attack caused by misbehaving CIoT UEs is depicted in figure 6.19.2.2-1.



Figure 6.19.2.2-1: AMF-based Mechanism to Mitigate DDoS Attack caused by CIoT UEs

1. CIoT UE was received a 5G-GUTI when the UE registered to the network.
2. – 2. The DF detects DDoS attack and outputs malicious UE IDs to the AMF.
3. The AMF stores the UE ID list in blacklist if the UEs are CIoT UEs. The AMF may setup a timer for the blacklist. When the timer is expired, the list shall be deleted. However, when the AMF is overloaded, the timer may be reset, extending the validity of the blacklist for another timer cycle.
4. When the AMF experiences to be overloaded, the AMF performs the mitigation procedures as described from step5 to step 8. However, when the AMF is still operating normally, e.g. DoS attack does not impact AMF performance, previous mitigation eased overloading, etc., the mitigation procedure shall not be performed.

NOTE 1: This mechanism is to protect the AMF from being overloaded caused by massive CIoT UEs. It is assumed that the misbehaving UEs will not move together, moved UEs will not significantly affect the other AMF. Thus, the blacklist is not needed to be shared with other AMF.

1. The AMF may trigger PDU session release procedure as depicted in clause 4.3.4 in TS 23.502 [15] to release the PDU session identified by the stored blacklist if the UE is in CONNECTED. The PDU Session Release Command may include a Back-off Timer, the UE shall not request to establish PDU session within the timer.
2. The UE who is commanded to trigger a DDoS attack may re-connect to the AMF. The UE sends NAS Request with GUTI to the AMF.
3. The AMF in overload case, compares 5G-GUTI with the blacklist, if the UE indicated by the 5G-GUTI is in the blacklist, the AMF shall reject the UE. If the 5G-GUTI is not in the blacklist, the RAN shall verify integrity of the NAS Request message to reject unauthorized UEs.
4. The AMF sends NAS Reject message to the UE with Back-off Timer, and the AMF will not waste resources to establish a PDU session with the misbehaving UE.

### 6.19.3 Evaluation

The solution fulfils the potential security requirements of KI#4. The 5G network entity, AMF could be able to protect itself from signalling overload.

When the AMF is overloaded, the AMF may control the misbehaving UEs received from DF, which means the AMF protects itself from signalling overload. The benefits and drawbacks are as follows:

**Benefits:**

1. Align with solution 17: No further changes in addition to solution 17.
2. Guarantee AMF usability: AMF can protect itself from draining resource massive malicious infrequent CIoT UE without any UE change.
3. Guarantee UE usability: DF cannot guarantee 100% precision, misinformation exists. In order to mitigate UE impact caused by the misinformation, the AMF will not launch the blacklist to isolate the UEs if the AMF it not overloaded. The solution will mitigate unnecessary complaint caused by misinformation.

**Drawbacks:**

The solution is used to protect AMF itself. Other NEs, e.g. RAN may not be protected, since RAN is in front of the AMF, and they have different computing capability.

**Efficiency:**

When the AMF needs to handle a group of misbehaving UEs, the AMF may trigger PDU session release procedure to release those UEs’ PDU session so that the UEs cannot deliver the DDoS flow. After that, the AMF will release misbehaving UEs’ PDU session level context, which reduces the storage burden for misbehaving UEs and provides more storage resources for the normal UEs. In order to avoid signalling overload caused by PDU session release message itself, the AMF should be implemented to disperse multiple release messages to different time slot.

## 6.20 Solution 20: RRC Connection Re-Establishment for the Control Plane for NB-IoT connected to 5GC

### 6.20.1 Introduction

This solution addresses the key issue #13 “Security for RRC Connection Re-Establishment for the Control Plane for NB-IoT connected to 5GC”.

When the UE re-establishes to the target RAN with S-TMSI, the RAN may not find the source AMF according to S-TMSI. In this case, the RAN may request a default target AMF to fetch UE context from the source AMF. Thus, context fetch between source AMF and target AMF is needed, and KAMF may be changed.

The solution proposes to reuse RRC Connection Re-Establishment for the Control Plane for NB-IoT connected to EPC when KAMF is not changed.

In addition, when the KAMF is changed, since it is a new security feature in 5G, the solution proposes to support key synchronization procedure.

### 6.20.2 Solution Details

#### 6.20.2.1 RRC Connection Re-Establishment Procedure without KAMF Change

In case that the KAMF is not changed, it is proposed to reuse solution depicted in clause 7.4.4 in TS 33.401 [7] for UE and AMF using Control Plane CIoT 5GS Optimisation. The solution is to request the AMF to authenticate the UE's RRC re-establishment request with UL\_NAS\_MAC since AS security is not activated, and is to request the UE to authenticate the AMF with DL\_NAS\_MAC when initiating the establishment of the UE's N2 connection with the RAN.

#### 6.20.2.2 RRC Connection Re-Establishment Procedure with KAMF Change

In case that the KAMF is changed, key synchronization procedure is introduced. Verification of DL\_NAS\_MAC is different from reused solution, but is backward compatible.



1. – 5, similar with current solution. The source AMF verifies UL-NAS-MAC calculated by the UE with KNAS-int, uplink NAS COUNT and target cell ID.
2. The source AMF decides to derive new KAMF\* according to local policy.
3. The source AMF responses UE’s context to the target AMF including KAMF\*.
4. Since new KAMF\* is derived, the target AMF shall derive new KNAS-int\*, and notify the UE with key derivation parameters, including K\_AMF\_change\_flag, the received downlink NAS COUNT, ngKSI, selected NAS security algorithms. DL\_NAS\_MAC\* shall be calculated with newly derived KNAS-int\* and these parameters in addition to target cell ID. Target cell ID is included to bind the target cell with target AMF because the UE cannot authenticate the target RAN without AS security context.
5. The target AMF sends key derivation parameters and DL\_NAS\_MAC\* to the target RAN.
6. The target RAN transparently sends the key derivation parameters and DL\_NAS\_MAC\* to the UE included in the RRCReestablishment message.
7. The UE shall derive new KAMF\* and KNAS-int\* according to received key derivation parameters.
8. The UE shall verify the DL\_NAS\_MAC\* with newly derived KNAS-int\* similar with calculation on the target AMF.
9. Once verification is successful, the UE shall reply RRCReestablishmentComplete message to the target RAN. The UE successfully re-establishes to the target RAN, and newly derived NAS key is used for the following data transmission.

### 6.20.3 Evaluation

The solution address key issue #13 “Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC”.

The solution reuses security handling for RRCConnectionReestablishment Procedure for Control Plane CIoT EPS optimisation.

While UE’s cell reselection due to RLF involves AMF change, the corresponding behavior for LTE (i.e., MME change in RRC connection reestablishment for NB-IoT CP optimization) has never been considered and therefore specified in RAN2 and SA2 working groups. Instead, TS 36.300 10.1.6 only describes the fallback procedure to idle when the UE context cannot be retrieved by the eNB.

Furthermore, when AMF change happens in RRC connection reestablishment, regardless of whether KAMF change happens or not, additional NAS signalling (e.g., 5G GUTI reallocation) is deemed necessary. The same applies to MME change in LTE. However, SA2 and RAN2 didn’t specify any optimized procedure for this case in TS 23.401 and TS 36.300 respectively. Note also that NB-IoT does not support the connected mode mobility procedure (i.e., handover), which implies mobility is not a main design consideration.

Considering the above, the RRC reestablishment procedure with KAMF change does not needs to be specified.

## 6.21 Solution 21: Protection of NAS Redirection Message

### 6.21.1 Introduction

This solution addresses the key issues #10 “Bidding down attack for NAS based redirection between core networks”.

The NAS Redirection message is not integrity protected, because the security context is not activated before sending it. It may cause bidding-down attack and DoS attack to the UE, and may lead to unavailable of 5G security enhancement feature, e.g. SUPI protection, initial NAS protection, etc.

Since the attack happens before security activation, the solution proposes to integrity protect the NAS Redirection message with a public key of AMF. In order to simply the key management, certificate is not used, instead, the Key pair to protect SUCI of home UDM is involved for the visited AMF to authorize its public key.

The solution is consisted of two procedures, Authorization Procedure and Protection Procedure of NAS message. When the AMF receives an initial NAS message from a UE, the AMF shall check whether it has a related valid authorized public key. If not, the AMF shall initiate Authorization Procedure with UE Authentication Procedure to require UDM to sign the public key for the AMF. If yes, the AMF could use the Public Key directly to protect potential unprotected downlink NAS message, e.g. NAS Redirection message.

### 6.21.2 Solution Details

#### 6.21.2.1 Procedure of Authorization for Public Key of the AMF



Figure 6.21.2.1-1: Procedure of Authorization for Public Key of the AMF

1. UE sends initial NAS message to the AMF, the message shall include SUCI.
2. If the AMF does not have a valid Public key PKAMF-PKx according to the public key mapping information (see step 8) for the UE, or the related Public key is expired, the AMF shall generate a pair of public key PKAMF-PKx and private key PRAMF-PKx.
3. The AMF finds AUSF according to SUCI. The AMF shall send Nausf\_UEAuthentication\_Authenticate Request with SUCI and its PKAMF-PKx to the AUSF.
4. The AUSF shall send Nudm\_UEAuthentication\_Get Request message to UDM with SUCI and PKAMF-PKx.
5. The UDM signs the PKAMF-PKx and expire time with its private key PRUDM related to PKUDM indicated in SUCI and signature algorithm indicated in sign alg, and gets the signature Sign (PKAMF-PKx). The expire time indicates the lifetime of the Sign (PKAMF-PKx), which can be configured locally.
6. The UDM responses Nudm\_UEAuthentication\_Get Response message to the AUSF, the message includes the Sign (PKAMF-PKx), sign alg and the expire time.
7. The AUSF responses Nausf\_UEAuthentication\_Authenticate Response message to the AMF, including the Sign (PKAMF-PKx), sign alg and the expire time.
8. The AMF shall store the public key mapping information, i.e., {Home PLMN ID + Routing ID + Public Key ID, PKAMF-PKx, PRAMF-PKx, sign alg, expire time, Sign (PKAMF-PKx)}.

#### 6.21.2.2 Procedure of Protection of NAS message



Figure 6.21.2.1-2: Procedure of Protection of NAS Redirection Message

1. UE sends initial NAS message to the AMF, the message may include SUCI or GUTI. NONCE1 is a freshness parameter from the ME, and also indicates to the AMF that the UE supports to verify integrity of the NAS Redirection message before security activation using public key. The ME may send this parameter when gets PKUDM from SIM card, SIM card may send the key to the UE when it inserts to the ME. PKUDM is the same key reused to protect SUCI.
2. If the AMF does not have a valid Public key PKAMF-PKx according to the public key mapping information for the UE, or the related Public key is expired, the AMF shall process as depicted in 6.21.2.1. Otherwise, the AMF could use the related Public key PKAMF-PKx to protect the NAS Redirection message. For example, if the UE ID is 5G-GUTI, the AMF finds PLMN ID, routing ID and Public Key ID in the UE context, and finds PKAMF-PKx, PRAMF-PKx, sign alg, expire time, Sign (PKAMF-PKx) according to the public key mapping information.
3. If the AMF wants to reject the UE when NAS security is not activated, the AMF shall generate NONCE2, and include NONCE1 and NONCE2 in the NAS Redirection message, the NONCE2 proves freshness from the network. The AMF shall sign the NAS Redirection message with PKAMF-PKx, and get Sign (NAS Redirection).
4. The AMF shall send NAS Redirection message to the UE including PKAMF-PKx, sign alg, expire time, Sign (PKAMF-PKx), NONCE1, NONCE2, and Sign (NAS Redirection).
5. On receiving the NAS Redirection message, firstly, the UE shall verify whether the Sign (PKAMF-PKx) is expired according to expire time. Secondly, the UE shall verify Sign (PKAMF-PKx) with UDM’s public key PKUDM. Finally, the UE shall verify Sign (NAS Redirection) with the PKAMF-PKx.

#### 6.21.2.3 Abnormal Cases

There are some corner cases that AMF cannot get Sign (PKAMF-PKx) from the UDM, e.g. roaming case, the visited PLMN has no roaming agreement with home PLMN. At this time, the visited AMF cannot contact the home UDM to get a sign (PKAMF-PKx). Thus, NAS Redirection message with cause#11 “PLMN not allowed” cannot be protected.

For these abnormal case, specific 5GMM cause is used, the UE will not verify integrity protection of the NAS Redirection messages with this specific 5GMM cause.

### 6.21.3 Evaluation

The solution addresses the key issues #11 “Bidding down attack for NAS based redirection between core networks”. The solution could also be used to protect the following NAS Reject message before NAS security is activated for CIoT UEs:

1. Registration Reject message
2. Service Reject message
3. Authentication Reject message
4. Deregistration Accept message

Except for:

Registration Reject message with cause “PLMN not allowed”, in case that vPLMN has no roaming agreement with hPLMN.

Legacy mechanism is defined in clause 5.3.20 in TS 24.501, however, it just specifies actions for the UE when receiving different 5GMM cause in NAS Reject message to mitigate the impact caused by non-integrity protected NAS Reject message. But the message could also be forged or tampered, the UE may still do some actions, e.g. delete/store PLMN, delete security context, etc.

With this solution, all the causes other than “PLMN not allowed” in NAS Reject can be integrity protected, which includes redirection to 4G. Moreover, if new feature is added in NAS Reject message, it could also be covered by this solution.

For CIoT UE, it is totally new in R16, so backward compatibility is not needed to be considered, feature negotiation is not needed. UE and network shall support this feature in the first release just like ABBA.

**UE Impact:**

SIM card shall be provisioned with a public key of UDM, which may be the same key to protect SUCI, SIM card is not impacted.

ME shall support DSS (e.g. FIPS 186-4) to verify integrity of NAS Reject message.

**RAN Impact:** none

**VPLMN impact:**

vAMF shall support generation and storage of public key pair.

vAMF shall support authorization procedure.

vAMF shall support DSS (e.g. FIPS 186-4) to sign NAS Reject message.

**HPLMN impact:**

hUDM shall support to authorization procedure.

hUDM shall support DSS (e.g. FIPS 186-4) to sign the public key from the AMF.

**Procedure impact:**

The solution reuses current authentication information request procedure to do authorization procedure.

The solution reuses current NAS Reject procedure to do NAS reject message protection.

The solution does not involve any new signalling overhead.

## 6.22 Solution #22: Security solution for UP IP in PDCP to protect UL EDT data in Msg 3

### 6.22.1 Introduction

This solution addresses key issue #2: Integrity protection of small data, key issue #3: Encryption of small data and key issue #8: Key and mac size for protection of small data in this TR.

This security solution address solution 19: 5GS UP Optimization for Infrequent Small Data Transmission in SA2 TR 23.724 [2]. This solution is to optimize small data transmission for the UEs from CM-IDLE mode. It enables transfer of user plane data without need for the Service Request procedure. According to solution 19 in SA2 TR 23.724 [2], it is proposed to keep AS context in the NG-RAN including information the UPF connection and relevant QoS flow(s) to be used for the connection, even when UE moves into CM-IDLE. When UE resumes the connection, the NG-RAN uses the information to activate DRB, AS security and User Plane connectivity over N3 for the small data packet delivery to the UPF.

In EPS/LTE Rel-15, early data transmission (EDT) feature was added to the RRC Connection Resume/Suspend procedures in eNB as specified in TS 33.401 [7]. Uplink user plane data is included as early data transmission with the RRC Connection Resume Request (msg 3). As described in TS 33.401 [7], the UE and the target eNB uses the newly derived KUPenc for ciphering/deciphering of the UL EDT data in LTE PDCP layer in the RRC Connection Resume Request message, and user DL data (if included) in PDCP layer in the RRC Connection Suspend or RRC Connection Resume message. Integrity protection of the UL EDT is not supported in Rel-15 in EPS.

This solution proposes to re-use the security solution for RRC Suspend and Resume procedures with EDT as defined in EPS/LTE Rel-15 in clause 7.2.11 in TS 33.401 [7] for E-UTRA connected to 5GC, with the following enhancements:

* For early data transmission (EDT) in RRC (Connection) Resume Request (i.e., msg 3), the UE applies the security policy of the DRB to the EDT data. If the user plane integrity protection is activated for the DRB to which the PDCP PDU (i.e., data) belongs, the UE derives the KUPint from the KgNB/Kng-eNB of the target cell and protects the integrity of the PDCP PDU using the selected integrity protection algorithm in the AS security context. If multiple PDCP PDUs are included in the RRC (Connection) Resume Request, each PDCP PDU is integrity protected based on the security policy for the respective DRB.

### 6.22.2 Solution details

#### 6.22.2.1 UL data transmission from CM-IDLE with Early Data Transmission

The following figure shows a single MO small data delivered from the UE using Early Data Transmission.



**Figure 6.22.2.1-1: Single MO data Transmission using 5GS UP Optimization and Early Data Transmission (EDT)**

Figure 6.22.2.1-1 shows the following steps:

1a. The UE sends RRC Connection Resume Request with the UL small data included as UL EDT (Early Data Transmission) data with the RRC Connection Resume Request (Msg 3) on SRB0 and hence it is not integrity protected. The UE includes information to be used for context identification and re-establishment in the RRC Connection Resume Request message: the Resume ID and a ShortResumeMAC-I.

For protection of the UL EDT data in the RRC Connection Resume Request message the description in clause TS 33.401 [7] for protection of EDT data is re-used with the following enhancements:

* The UE is integrity protecting the UL EDT data in PDCP protocol using a newly derived KUPint if configured in PDCP.
* The target RAN verifies the MAC-I included in PDCP protocol protecting the UL EDT data after the target RAN has retrieved the UE security context from the source RAN. The target RAN then verifies the integrity of the UL EDT data using the newly derived KUPint

1b. The RAN immediately suspends the RRC connection (to minimize UE power consumption) as described in TS 23.724 [2].

2. The RAN forwards the UL data received from the UE to the UPF as described in TS 23.724 [2].

3. UE and RAN remain suspended as described in TS 23.724 [2].

#### 6.22.2.2 Connection Suspend procedure using the Early Data Transmission (EDT) feature

This procedure is used by the RAN to suspend the connection if 5GS UP Optimization is supported as described in solution 19 in TS 23.724 [2].

It is expected that the security solution defined in clause 7.2.11 in TS 33.401 [7] for EDT is re-used for this scenario.

### 6.22.3 Evaluation

This solution proposes that the UL EDT data multiplexed with Msg 3 is integrity protected in PDCP protocol. This solution resolves key issue #2.

SA3 is currently studying UP IP in the ongoing study in TR 33.853 for Rel-16. If UP IP is introduced in LTE PDCP and RAN2 concludes to use LTE PDCP in eMTC connected to 5GC, then UL EDT data could be integrity protected in either LTE PDCP or NR PDCP.

## 6.23 Solution #23: Mitigate DDoS Attack on RAN based on RANs coordination

### 6.23.1 Introduction

This solution addresses the key issue #5 “gNB Protection from CIoT DoS attack”.

More and More IoT terminals support mobility such as police or military terminals, Smart Automated Cars etc. Mobility-enabled terminals could be compromised to perform similar actions at the same time and cause a RRC signalling attack to the RAN. Since the terminals move fast, the neighbour RAN may be impact.

The RAN could identify misbehaving UEs by traffic statistics detection mechanism itself which takes time, so, the misbehaving UE lists should be distributed to its neighbour RANs to shorten detecting time. Then if the misbehaving UEs move to neighbour RAN, the neighbour RAN could use the list to protect itself from DoS attack.

### 6.23.2 Solution details

Misbehaving UEs may send malicious RRC signalling to the RAN trying to trigger a DoS attack to the RAN, the RAN identifies misbehaving UEs by itself based on traffic statistics detection mechanism, e.g. similar as solution 7. In order to provide protection for the neighbour RAN and try to shorten detecting time of the neighbour RAN, the original RAN reports the misbehaving UE ID list, e.g. C-RNTI/ResumeID lists to its neighbour RANs.

The neighbour RANs could either use the result directly, or use it as a reference to identify the misbehaving UE, with this list, the RAN could handle the misbehaving UE lists with already defined RAN access control mechanism, e.g. RRC Release or Reject procedure based on current RAN operation state, e.g. CPU usage, etc.

### 6.23.3 Evaluation

This solution provides a mechanism to mitigate the DoS attack on RAN when mobility-enabled IoT UEs are compromised to launch attack.

Editor’s note: How to synchronize the list within RANs is FFS.

## 6.24 Solution #24: Using NAS security for protection of NAS Redirection message

### 6.24.1 Introduction

This solution addresses key issue #11: Bidding down attack for NAS based redirection between core networks.

This solution proposes that AMF establishes NAS security with the UE to be able to protect the NAS Redirection message to the UE and the UE should only act upon the NAS Redirection message upon on a successfully integrity protected NAS Redirection message.

### 6.24.2 Solution details

The solution is to simply protect the NAS Redirection messages that are used to redirect the UE to another system. When the AMF wants to send the NAS Redirection message to the UE, then the AMF establishes NAS security with the UE, if NAS security is not already established, and the AMF applies the NAS security to the NAS Redirection message. The UE only acts upon the NAS Redirection message if its integrity protected and the UE verifies the integrity successful.

NOTE: This solution does not apply to unauthenticated emergency calls.

### 6.24.3 Evaluation

The solution fulfils the requirement in key issue #11.

The impact of the solution is to require the AMF to establish NAS security with the UE and protect the NAS Redirection message to the UE and the UE to only act based on verifying the integrity of the NAS Redirection message successfully.

TS 33.501 [8] Rel-16 contains already a solution where the AMF is required to protect NAS messages that modify the CAG list in the UE and the UE to only modify the CAG list based on a successfully integrity protected NAS message.

Also, the security solution in EPC/LTE requires the MME to establish NAS security with the UE in certain error cases, if feasible, in order to be able to integrity protect Attach Reject and Tracking Area Update Reject messages including reject causes. Requiring the AMF to establish NAS security to protect Registration Reject messages with certain EMM causes, was never an issue in EPC/LTE systems.

Also, if the Registration Request message is sent with no protection, then the Registration Request message includes a limited number of IE’s that are allowed to be sent without protection. The AMF may need to establish NAS security anyway in order to request the complete Registration Request message in NAS Security Mode Command.

## 6.25 Solution #25: Security solution for preventing Botnet Attacks from Improper CIOT Device Use

### 6.25.1 Introduction

This solution addresses key issue #x: preventing Botnet Attacks from Improper CIOT Device Usage. This solution is proposing enabling the serving network to be aware of CIOT devices expected behaviour. This solution provides the serving network this information by utilizing IETF RFC 8520 which specifies the Manufacturers Usage Description (MUD) protocol. MUD provides a scalable and efficient solution for communicating detailed networking requirements to local network devices in a machine-readable format. This information is sufficient for network devices to create per-device white and blacklists. However, the IETF did not address cellular IOT devices. This document identifies three potential options for communicating networking requirements to cellular networks using MUD. The MUD protocol is designed to enable a CIOT device to signal to the network the types of access and functionality it requires to properly operate. This information is provided from the device in the form of a MUD URL as specified in IETF RFC8520. The ability for networks to be aware and constrain the communication abilities of exploited IoT devices reduces the potential for the devices to be used in attacks—both DDoS attacks that could be launched across the internet and attacks on the IoT device’s local network that could have security consequences.

The IETF MUD RFC provides a mechanism for signalling a standardized way for a CIOT device to signal this information to the serving network. A simple example of this capability is as follows;

“A light bulb is intended to light a room. It may be remotely controlled through the network, and it may make use of a rendezvous service (which could be accessed by an application on a smart phone). What we can say about that light bulb, then, is that all other network access is unwanted. It will not contact a news service, nor speak to the refrigerator, and it has no need of a printer or other devices. It has no social networking friends. Therefore, applying an access list to it that states it will only connect to the single rendezvous service will not impede performing its function; at the same time, this will allow the network to provide the light bulb and other devices an additional layer of protection. [1]”

### 6.25.2 Solution A details

The CIOT device sends the MUD URL specified in IETF RFC8520 as part of the UE network capability information element.

### 6.25.2 Solution B details

The Home network delivers the MUD URL specified in IETF RFC8520 to the serving network upon successful attach of the CIOT device. The information regarding the CIOT device’s expected usage is available to the home network based on the IMSI and subscription information.

### 6.25.2 Solution C details

The serving network retrieves the MUD URL specified in IETF RFC8520 based on the IMEI. The information is available to the serving network through a central repository. This repository could be built in collaboration with GSMA by including the MUD URL in the TAC table of the IMEI database.

Botnets have not been known to change the IMEI of compromised IoT devices because they only operate within the main processor and not the modem itself, therefore it makes sense to have an understanding of a devices expected network usage based on IMEI by the serving network.

NWDAF could then make use of the MUD information to detect whether a device or a set of devices is deviating from its expected behaviour.

### 6.25.3 Evaluation

Solutions utilizing the IETF RFC 8520 Manufacturers Usage Description (MUD) protocol may meet the potential security requirement to support detection of UE misbehaviour.

The different alternatives presented in this solution describes different approaches on how to leverage the IETF RFC 8520 Manufacturers Usage Description (MUD) protocol in the 5GS. All solutions proposed leaves out how to integrate the MUD protocol into the 5GS for further study. These clarifications on integration are essential to be able to properly determine the potential architectural impact and gained value to the 5GS by introducing the IETF RFC 8520 Manufacturers Usage Description (MUD) protocol.

## 6.26 Solution #26: Hash based UE capability protection for CP optimization only CIoT UE

### 6.26.1 Introduction

This solution addresses key issue #15: Security for UE radio capability transfer for CIoT UE.

### 6.26.2 Solution details

This solution proposes to protect the UE radio capabilities of control-plane only CIoT UEs in the following way.

1. UE includes the hash of its radio capabilities in the Registration Request message to the network
2. The network verifies the UE radio capabilities when it acquires the UE radio capabilities as part of the UE capability enquiry procedure

The procedure below only shows the messages required for the UE radio capability verification.



Figure 6.26.2-1: UE Radio Capability verification procedure for CP only CIoT devices

1. UE sends a Registration Request message with Hash of the UE radio capabilities (Hash\_RC).

Editor’s Note: How the Hash\_RC in the initial Registration Request is protected is FFS.

Editor’s Note: How often hash needs to be calculated is FFS.

2. AMF determines to trigger a UE radio capability enquiry procedure by sending a UE radio capability information request message with the received Hash\_RC to NG-RAN node serving the UE.

Editor’s Note: How often the UE radio capability info request is triggered by AMF is FFS.

3. The NG-RAN node performs UE Capability Enquiry procedure with the UE to get the UE radio capabilities.

Editor’s Note: Whether the solution allows early acquision of UE radio capability by NG-RAN node should be clarified.

4. The NG-RAN node calculates the hash of the received UE radio capabilities and compares the calculated hash value with the Hash\_RC. If they match, the NG-RAN node stores the UE capabilities with a verified flag set.

5. After successful verification of the UE radio capability, the NG-RAN node sends the UE radio capabilities to the AMF with an indication of successful verification.

6. The AMF stores the UE radio capabilities with a verified flag set.

NOTE: The verified flag can be used by the upgraded AMF (i.e., AMF that understands the verified flag) to confirm that the UE radio capability has already verified by another AMF when it receives the UE radio capability from a legacy AMF or NG-RAN node.

Editor’s Note: RAN impacts of this solution is FFS.

### 6.26.3 Evaluation

TBD

## 6.27 Solution #27: Network resilience for UEs without AS security

### 6.27.1 Introduction

This solution addresses the key issue #15, Protection of UE capability transfer for UEs without AS security.

### 6.27.2 Solution details

When handling UEs that do not support AS security, the NG-RAN that had acquired UE capabilities from those UEs using RRC UE capability transfer procedure should not store them locally for long duration and shall not send them to other network entities. The NG-RAN may re-use those UE capabilities within this duration. The setting for this duration is left up to the implementations and network/operator policy.

Doing so does not require any change to these optimized UEs and sufficiently ensures that any tampering of UE capabilities over-the-air does not have persistent/long-lasting effect on the network side.

### 6.27.3 Evaluation

TBD

## 6.28 Solution #28: Protection of UE capability transfer for UEs without AS security

### 6.28.1 Introduction

This solution addresses key issue #15: Security for UE radio capability transfer for CIoT UE.

### 6.28.2 Solution details

This solution proposes to protect the UE radio capabilities of CIoT UEs without AS security in the following way.

1. AMF checks if UE radio capability info is required;
2. NAS security is used to protect the UE radio capability info request and response message.



Figure 6.28.2-1: UE Radio Capability verification procedure for CP only CIoT devices

1. UE sends a Registration Request message to AMF.

2. If UE radio capability info is required, AMF determines to trigger a UE radio capability enquiry procedure.

3. AMF checks if it is a CIoT UE that only support CP optimization. If yes, AMF sends a UE radio capability information request message with NAS security protection.

4. After successful verification of the received DL NAS message, UE sends the UE radio capabilities to the AMF with NAS security protection

5. AMF stores the UE Capability information during CM IDLE state for the UE and RM-REGISTERED state for the UE after successful verification. The AMF deletes the UE radio capability when the UE RM state in the AMF transitions to RM-DEREGISTERED.

6. AMF sends its most up to date UE Radio Capability information to the RAN in the N2 REQUEST message when needed.

### 6.28.3 Evaluation

Editor’s Note: Early UE capability requiring is FFS

Editor’s Note: feasibility of stoluion is FFS.

Editor’s Note: System impact is FFS.

## 6.29 Solution #29: Security solution for UE Capability Transfer for UE with no AS security.

### 6.29.1 Introduction

This solution addresses key issue #15: Security Protection for UE capability transfer in this TR.

UE using CIOT CP optimization does not have AS security establishment. As a result, the existing solutions for normal UEs to protect the UE capability transfer does not prevent tampering of UE capability transfer using MITM attack as described in key issue detail of Key Issue #15.

This solution proposes to use the NAS based keys to protect the UE capability transfer from UE to the core network.

### 6.29.2 Solution details



**Figure 6.Y.2.1: UE Capability Transfer for UEs with No AS Security.**

1. The network initiates the UE capability enquiry procedure to a UE in RRC\_CONNECTED when it needs (additional) UE radio access capability information.

* 1. Upon receiving the UE capability enquiry, UE calculates UL\_MAC for UE capability information using KNAS\_INT and currently used the NAS integrity algorithm and a counter.
  2. UE sends the UE capability information message to RAN along with UL\_MAC .  
     Note: UE modelling to handle UL and DL MAC should be left to RAN2 and CT groups.

Editor’s Note: Effects of RAN to AMF call flow are FFS.

Editor’s Note: Figure needs to be updated to match steps in the description.

1. RAN forwards the UL\_MAC, counter, to the core network for verification. Upon successful verification, the network sends decrypted capability information and notification to RAN. Upon successful verification, AMF stores the verified radio capability information.

### 6.29.3 Evaluation

## 6.30 Solution #30: AMF verification of the UE radio capabilities for CP optimization only CIoT UE

### 6.30.1 Introduction

This solution addresses key issue #15: Security for UE radio capability transfer for CIoT UE.

### 6.30.2 Solution details

This solution proposes to protect the UE radio capabilities of control-plane only CIoT UEs in the following way.

1. UE includes the hash of its radio capabilities in the Registration Request message to the network
2. AMF verifies the UE radio capabilities when it acquires the UE radio capabilities based on the UE capability enquiry procedure

The procedure below only shows the messages required for the UE radio capability verification.



Figure 6.y.2-1: UE Radio Capability verification procedure for CP only CIoT devices

1. UE sends a Registration Request message with Hash of the UE radio capabilities (Hash\_RC).

Editor’s Note: How the Hash\_RC in the initial Registration Request is protected is FFS.

2. AMF determines to trigger a UE radio capability enquiry procedure by sending a UE radio capability information request message with the received Hash\_RC to NG-RAN node serving the UE.

Editor’s Note: How often the UE radio capability info request is triggered by AMF is FFS.

3. The NG-RAN node performs UE Capability Enquiry procedure with the UE to get the UE radio capabilities.

Editor’s Note: Whether the solution allows early acquision of UE radio capability by NG-RAN node should be clarified.

4. The NG-RAN node sends the UE radio capabilities to the AMF.

5. The AMF calculates the hash of the received UE radio capabilities and compares it with the hash received from the UE. If they match (i.e., verification is successful), the AMF stores the UE radio capabilities with a verified flag set.

NOTE 1: The verified flag can be used by the upgraded AMF (i.e., AMF that understands the verified flag) to confirm that the UE radio capability has already verified by another AMF when it receives the UE radio capability from a legacy AMF.

NOTE 2: If hash verification fails, the AMF would throw the UE Radio capabilities away. In this case, the UE radio capabilities would need to be re-fetched at the next connection.

### 6.30.3 Evaluation

## TBD6.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 that will form the basis for any normative work.

## 7.1 Key Issue #1: Efficient frequent small data transmissions

It is agreed that the size of the MAC fields or the length of the keys cannot be reduced. Since no relevant performance issues were identified with the Release 15 security mechanisms, it is concluded that no normative work is required for this key issue.

## 7.2 Key Issue 2: Integrity protection of small data

Solution 1 is recommended for normative work to support integrity protection for infrequent small data transmission via NAS signaling.

For integrity protection of EDT data, given that RAN2 has decided not to specify NR PDCP for NB-IoT and instead to align as much as possible with the mechanisms in the EPS solution, it is concluded that no normative work is to be done in Release 16.

## 7.3 Key Issue 3: Encryption of small data

Solution 1 is recommended for normative work to support encryption for infrequent small data transmission via NAS signaling.

Solution 18 is recommended for normative work to support encryption of Mobile Originated EDT data.

## 7.4 Key Issue 4: Signalling overload due to Malicious Applications on the UE

It is concluded that for KI#4 no normative work is needed for Rel-16.

## 7.5 Key Issue 5: gNB Protection from CIoT DoS attack

It is concluded that for KI#5 no normative work is needed for Rel-16.

## 7.6 Key Issue 6: Avoiding AS security for application security enabled UEs.

It is concluded that for KI#6 no normative work is needed.

## 7.7 Key Issue 7: Key refreshing for protection of small data

Existing mechanisms in TS 33.501[8] can be used for key refreshing and keys can be refreshed based on local configuration, operator policy etc., taking into account the small data characteristics. It is concluded that for KI#7 no normative work is needed as existing mechanisms are sufficient.

## 7.8 Key Issue 8: Key and mac size for protection of small data

It is concluded that for KI#8 no normative work is needed. The current size of keys and MAC shall be reused for CIoT.

## 7.9 Key Issue 9: Protection of NIDD interfaces

Solution 8 is recommended for normative work to support protection of NIDD interfaces.

## 7.10 Key Issue 10: User Plane data transmission with Connectionless signalling.

It is concluded that for KI#10 no normative work is needed.

## 7.11 Key Issue 11: Bidding down attack for NAS based redirection between core networks

Solution #24 is recommended for normative work to support NAS security for protection of NAS Redirection message between 5GS and EPC.

## 7.12 Key Issue 12: Privacy protection of new parameters for CIoT included in NAS message

No normative work is required for addressing Key Issue #12.

## 7.13 Key Issue 13: Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC

Reused solution depicted in clause 6.20.2.1 is recommended for normative work for Security Handling in RRC Connection Re-Establishment for the control plane for NB-IoT connected to 5GC when the KAMF is not changed.

## 7.14 Key Issue 14: Preventing User Plane Botnet Attacks from Improper CIOT Device Usage

No normative work is to be done for addressing Key Issue #14.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2018-05 | SA3#91bis | S3-181853 |  |  |  | TR skeleton | 0.0.0 |
| 2018-05 | SA3#91bis | S3-182079 |  |  |  | Version after SA3#91bis incorporating changes from S3-182078. | 0.1.0 |
| 2018-09 | SA3#92 ad-hoc | S3-183068 |  |  |  | Version after incorporating changes from S3-183132, S3-183133, S3-183134, S3-183135, S3-183136, S3-183170, S3-183171, S3-183173, S3-183176 | 0.2.0 |
| 2018-11 | SA3#93 | S3-183774 |  |  |  | Version after incorporating changes from S3-183772, S3-183773, S3-183775, S3-183777, S3-183778, S3-183779, S3-183780, S3-183781, S3-183782, S3-183783 | 0.3.0 |
| 2019-02 | SA3#94 | S3-190471 |  |  |  | Version after incorporating changes from S3-190075, S3-190077, S3-190195, S3-190271, S3-190470, S3-190472, S3-190473, S3-190474, S3-190475, S3-190476, S3-190479, S3-190480, S3-190481, S3-190482, S3-190483, S3-190484, S3-190485, S3-190486, S3-190488, S3-190489, S3-190490 | 0.4.0 |
| 2019-03 | SA3#94-Ad hoc | S3-191026 |  |  |  | Version after incorporating changes from S3-190717, S3-190662, S3-190784, S3-190785, S3-190792, S3-190815, S3-190817, S3-191027, S3-191025, S3-191028, S3-191032, S3-191033 and S3-191029 | 0.5.0 |
| 2019-03 | SA#83 | SP-190105 |  |  |  | Presented for information | 1.0.0 |
| 2019-05 | SA3#95 | S3-191677 |  |  |  | Version after incorporating changes from S3-191676, S3-191678, S3-191679, S3-191680, S3-191681, S3-191682, S3-191683, S3-191684, S3-191685, S3-191686, S3-191687, S3-191688 and S3-191689 | 1.1.0 |
| 2019-06 | SA3#95bis | S3-192392 |  |  |  | Version after incorporating changes from S3-191810, S3-191876, S3-191893, S3-192071, S3-192105, S3-192106, S3-192398, S3-192400, S3-192401, S3-192452, S3-192393, S3-192399, S3-192402 and S3-192404 | 1.2.0 |
| 2019-08 | SA3#96 | S3-193103 |  |  |  | Version after incorporating changes from S3-192538, S3-192771, S3-192896, S3-192897, S3-192939, S3-192967, S3-193102, S3-193106, S3-193108, S3-193101, S3-193104, S3-193105, S3-193107 | 1.3.0 |
| 2019-10 | SA3#96-Ad hoc | S3-193703 |  |  |  | Version after incorporating changes from S3-193537, S3-193538, S3-193542, S3-193543, S3-193545, S3-193547, S3-193711, S3-193712, S3-193713, S3-193714, S3-193539, S3-193843 | 1.4.0 |
| 2019-11 | SA3#97 | S3-194489 |  |  |  | Version after incorporating changes from S3-194491, S3-194233, S3-194234, S3-194240, S3-194490, S3-194492, S3-194498, S3-194604, S3-194497, S3-194239, S3.194493 S3-194494 and S3-194495 | 1.5.0 |
| 2020-05 | SA3#99-e | S3-193103 |  |  |  | Version after incorporating changes from S3-201383 and S3-201037 | 1.6.0 |