|  |  |
| --- | --- |
| 3GPP TR 33.700-29 V0.3.0 (2024-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of 5G Satellite Access  in the 5G architecture;  Phase 3  (Release 19) | |
|  | |
|  |  |
|  | |
| 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.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms and abbreviations 9

3.1 Terms 9

3.2 Abbreviations 9

4 Architecture and security assumptions 9

5 Key issues 9

5.1 Key Issue #1: Security protection in Store and Forward Satellite Operation 10

5.1.1 Key issue details 10

5.1.2 Security threats 10

5.1.3 Potential security requirements 11

5.2 Key Issue #2: Key Issue on privacy threats in S&F operation 11

5.2.1 Key issue details 11

5.2.2 Security threats 11

5.2.3 Potential security requirements 11

5.X Key Issue #X: <Key Issue Name> 12

5.X.1 Key issue details 12

5.X.2 Security threats 12

5.X.3 Potential security requirements 12

6 Solutions 12

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: Inverse AKA 12

6.1.1 Introduction 12

6.1.2 Solution details 12

6.1.2.1 Solution details for S&F in EPS 13

6.1.2.2 Solution details for S&F in 5G 14

6.1.3 Evaluation 16

6.2 Solution #2: IOPS security concept for S&F 17

6.2.1 Introduction 17

6.2.2 Solution details 17

6.2.2.1 Solution details for S&F in EPS 17

6.2.2.2 Solution details for S&F in 5G 19

6.2.3 Evaluation 20

6.3 Solution #3: IOPs based solution for UE to satellite security 20

6.3.1 Introduction 20

6.3.2 Solution details 21

6.3.3 Evaluation 21

6.4 Solution #4: Store and forward satellite operation 21

6.4.1 Introduction 21

6.4.2 Solution details 22

6.4.3 Evaluation 25

6.5 Solution #5: Onboard UDM 25

6.5.1 Introduction 25

6.5.2 Solution details 25

6.5.3 Evaluation 26

6.6 Solution #6: Primary authentication and NAS security context establishment during store-and-forward operations 26

6.6.1 Introduction 26

6.6.2 Solution details 27

6.6.3 Evaluation 28

6.7 Solution #7: Optimization of subsequent authentication procedure in S&F operation 28

6.7.1 Introduction 28

6.7.2 Solution details 28

6.7.2.1 Provisioning of authentication vectors 28

6.7.2.2 Optimized subsequent authentication procedure 29

6.7.3 Evaluation 31

6.8 Solution #8: Solution on preventing DoS attacks in S&F operation 31

6.8.1 Introduction 31

6.8.2 Solution details 32

6.8.3 Evaluation 33

6.9 Solution #9: Secure Initial Registration for S&F satellite operation 34

6.9.1 Introduction 34

6.9.2 Solution details 34

6.9.3 Evaluation 35

6.10 Solution #10: UE Attach/Registration method for S&F operation 35

6.10.1 Introduction 35

6.10.2 Solution details 36

6.10.3 Evaluation 37

6.11 Solution #11: UE context management for S&F operation 37

6.11.1 Introduction 37

6.11.2 Solution details 37

6.11.3 Evaluation 38

6.12 Solution #12: Authentication for store and forward satellite operation 39

6.12.1 Introduction 39

6.12.2 Solution details 40

6.12.3 Evaluation 41

6.13 Solution #13: Security protection based on onboard HSS 41

6.13.1 Introduction 41

6.13.2 Solution details 41

6.13.3 Evaluation 42

6.14 Solution #14: Authorization mechanism for uplink NAS message in S&F satellite operation 42

6.14.1 Introduction 42

6.14.2 Solution details 42

6.14.3 Evaluation 43

6.15 Solution #15: Attach procedure with eNB on board the satellite 44

6.15.1 Introduction 44

6.15.2 Solution details 45

6.15.3 Evaluation 46

6.16 Solution #16: Authorization during S&F MO transmission 46

6.16.1 Introduction 46

6.16.2 Solution details 47

6.16.3 Evaluation 47

6.17 Solution #17: Attach procedure with MME on board the satellite 48

6.17.1 Introduction 48

6.17.2 Solution details 48

6.17.3 Evaluation 49

6.18 Solution #18: Security protection for store and forward satellite operation 49

6.18.1 Introduction 49

6.18.2 Solution details 49

6.18.3 Evaluation 49

6.19 Solution #19: Mitigating UE privacy risks using temporary UE ID 49

6.19.1 Introduction 49

6.19.2 Solution details 50

6.19.3 Evaluation 51

6.20 Solution #20: Mitigation of privacy issues of interim GUTI 51

6.20.1 Introduction 51

6.20.2 Solution details 52

6.20.2.1 Alternative 1: restrict the use of interim GUTI 53

6.20.2.2 Alternative 2: No use of interim GUTI 53

6.20.3 Evaluation 53

6.21 Solution #21: Remediation of unauthenticated (D)DOS in S&F 53

6.21.1 Introduction 53

6.21.2 Details 54

6.21.2.1 Puzzles 56

Solving an Encryption Reversing puzzle example 56

Solving a one-way cryptographic hash function reversing puzzle example 58

6.21.3 Evaluation 60

6.22 Solution #22: AS security context establishment with store-and-forward operations 60

6.22.1 Introduction 60

6.22.2 Solution details 60

6.22.3 Evaluation 63

6.23 Solution #23: Security protection in S&F satellite operation with RAN on board 63

6.23.1 Introduction 63

6.23.2 Solution details 64

6.23.3 Evaluation 65

6.24 Solution #24: Expedited Authentication in 5GS in S&F Mode 65

6.24.1 Introduction 65

6.24.2 Solution details 66

6.24.3 Evaluation 68

6.25 Solution #25: Solution on preventing DoS attacks before security context is established 68

6.25.1 Introduction 68

6.25.2 Solution details 69

6.25.3 Evaluation 70

6.26 Solution #26: Protection of partial registration or attach accept message in S&F operation 71

6.26.1 Introduction 71

6.26.2 Solution details 71

6.26.3 Evaluation 72

6.Y Solution #Y: <Solution Name> 72

6.Y.1 Introduction 72

6.Y.2 Solution details 72

6.Y.3 Evaluation 72

7 Conclusions 72

7.Z Key Issue #Z: <Key Issue Name> 72

Annex <A>: <Informative annex title for a Technical Report> 73

Annex <X>: Change history 74

# 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.

# 1 Scope

The present document studies the security and privacy aspects of 5G satellite access phase 3. It is comprised of the following parts:

- Identify and study the security and privacy key issues of the regenerative payload generic architecture in 5GS/EPS.

- Identify and study the security and privacy key issues of the Store and Forward (S&F) Satellite operation both for NR NTN (5GS) and for IoT NTN (EPS).

- Identify and study the security and privacy key issues of UE-Satellite-UE communication enhancements for 5GS.

- The impact on regulatory services in the context of 5G satellite access. In particular, the assessment of the potential impact to lawful intercept in regenerative, Store and Forward (S&F), and UE-satellite-UE communication enhancement architecture.

# 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 23.700-29: "Study on integration of satellite components in the 5G architecture; Phase 3".

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

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[6] 3GPP TS 33.210: "Network Domain Security- (NDS): IP network layer security".

[7] 3GPP TS 33.102: "3G security; Security architecture".

[8] IETF RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".

[9] 3GPP TS 23.401: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"

…

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

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], 3GPP TR 23.700-29[2] 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.

## 3.2 Abbreviations

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

S&F Store and Forward

# 4 Architecture and security assumptions

The following architecture and security assumptions are applied to the study:

- The architecture assumptions and principles for EPS/5GS integrating of satellite components as defined in TR 23.700-29 [2] are used as architecture assumptions in this study.

- The security architecture, procedures, and security requirements for EPS/5GS as defined in TS 33.401 [3] / TS 33.501 [4] are used as a baseline.

- The IP Multimedia Subsystem (IMS) media plane security as defined in TS 33.328 [5] is used as a baseline.

- The physical security of 3GPP systems on board orbiting satellites is out of the scope of 3GPP.

- The feeder link and the inter-satellite link (ISL) are assumed to act only as transport layer links and are not specified in 3GPP.

- The use of feeder link and ISL is assumed to have no impact on the security of reference points (including the X2/Xn interface, S1-MME/N1 interface, S1-U/N3 interface, and the interfaces between the core network entities) by using the network domain security as defined in TS 33.210 [6].

- The security environment of 3GPP systems on board orbiting satellites is dependent on implementation and operation’s policy.

- Native IP-based communication protocol (as defined in TS 33.210 [6]) security at the network layer can be used to secure the IP transport connectivity available over the feeder link and the inter-satellite link (ISL) satellite transport links.

Editor’s Note: The priority of the security study between IoT NTN (EPS) and NR NTN (5GS) and the scenario when two UEs are under the coverage of the same satellite are to be aligned with TR 23.700-29 [2]. The security study should be aligned with TR 23.700-29 [2].

# 5 Key issues

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

## 5.1 Key Issue #1: Security protection in Store and Forward Satellite Operation

### 5.1.1 Key issue details

In clause 4 of TR 23.700-29 [2], there is following description about the Store and Forward Satellite Operation:

*"The following architecture assumptions are applied to the study:*

*…*

*- Store and Forward Satellite Operation assumes that UE-satellite-ground network connectivity can be intermittent as defined in clause 3.1.*

*- Store and Forward Satellite Operation shall work without ISL.*

*…"*

From a security perspective, whether a UE can use Store and Forward Satellite service should be assured by the 3GPP network.

In S&F satellite operations, architectural assumption is that the UE-satellite-ground network connectivity is intermittent. 3GPP Network Functions and/or Network Elements which are located on a satellite may communicate with the ground infrastructure of 3GPP network over an intermittently available feeder link connection between the satellite and the ground network. S&F satellite operational mode is relevant for delay tolerant and non-real time communications via LEO/MEO space segment.

During the feeder link’s intermittent unavailability, the following risks arise.

1. The EPS/5G AKA procedure may not get fully completed or is partially completed. It results into incomplete procedure for mutual authentication between the network and the UE.

2. The Security Mode Command (SMC) procedure for Non-Access Stratum (NAS) may not fully complete because the NAS connection between UE and MME/AMF may have been interrupted. In turn it results into incomplete security capabilities negotiation between the UE and the EPS/5GC network.

This key issue is to study the authentication, authorization and data security in Store and Forward Satellite Operation.

### 5.1.2 Security threats

Due to the nature of the S&F mode during the feeder link’s intermittent unavailability, the following threats can manifest themselves:

- When the UE and 3GPP network cannot mutually authenticate, this condition may cause issues such as Man-in-the-Middle (MITM) or impersonation attacks.

- Without authentication, confidentiality, integrity, and anti-replay protection there will be no security protection of the communication between UE, 3GPP system on board satellite, and ground-based 3GPP systems.

For the uplink control plane data (e.g. NAS message) and user plane data (e.g. if integrity protection is not activated), the 3GPP systems on board the satellite are not able to verify its integrity. It is hard to detect whether the data is sent from a genuine UE or an attacker. All the uplink data needs to be stored during the feeder or ISL links’ period of unavailability. Hence, the storage capacity can be easily exhausted by spoofed data with the attack over the air. This issue is amplified by the inability to upgrade hardware (e.g., radios, memory) on board of satellite. As an example, in case of the incomplete AKA procedure, user-plane data or control-plane data from unauthorized UE, the storage resource of on board satellite 3GPP system may be exhausted, resulting in the denial of service (DoS) attack.

NOTE: The risk of resource depletion of the 3GPP system is dependent on the agreed architecture solution direction of S&F KI in TR 23.700-29 [2].

### 5.1.3 Potential security requirements

The 3GPP system shall support mutual authentication between the UE and the 3GPP network in the Store and Forward Satellite Operation.

The 3GPP system shall support means to provide confidentiality, integrity, and anti-replay protection for user-plane and control-plane messages between UE and the 3GPP network in the Store and Forward Satellite Operation.

The 3GPP system shall support means to mitigate the potential denial of service attack in the Store and Forward Satellite Operation.

NOTE: The security requirements apply to all the potential store & forward architecture options in TR 23.700-29 [2], i.e. RAN-only on-board, RAN and partical-CN on-board, RAN and CN on-board.

Editor’s Note: whether there are more security requirements is FFS.

## 5.2 Key Issue #2: Key Issue on privacy threats in S&F operation

### 5.2.1 Key issue details

In satellite S&F scenario, when a UE attaches or registers to the network (when service link is available) via on-board eNB/gNB and NFs the satellite supporting S&F operation stores the registration request until the feeder link is available and sends an interim response message to the UE. Due to unavailability of the feeder link, the UE may not get authenticated (until the feeder link is available) and establish the security context to protect the response messages.

In such scenarios, the on-board eNB/gNB and MME/AMF should ensure security and privacy of the UE, by protecting the response message which might include sensitive information of the UE (for example, assignment of temp ID in the response message). If any UE related information is sent in clear text there is a possible attack of UE traceability and linkability security threats.

In this key issue it is proposed to study potential solution to prevent the UE and on-board eNB/gNB and NFs from sharing information in clear over the air, which might lead to privacy threats.

NOTE: The privacy threats of the 3GPP system in S&F is dependent on the final agreed architecture solution direction of S&F KI in TR 23.700-29 [2].

### 5.2.2 Security threats

As an example, scenario if the UE tries to attach/registers when service link is available, it is possible that the on-board satellite rejects or partially accepts the request by storing the request in S&F buffer. The on-board satellite sends reject or partial accept message which is unprotected as the UE and the network side are not authenticated and established the NAS/AS security association yet. In such scenario including a reject cause or any (interim) temporary identifier may allow the attacker to track the UE.

Editor's Note: Whether a reject cause or any (interim) temporary identifier can be used by the attacker to track the UE is FFS.

### 5.2.3 Potential security requirements

The 3GPP system shall support means to mitigate the potential linkability and trackability attack on UE in the Store and Forward Satellite Operation.

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | | |
| Solutions | 1 | 2 |  |  |  |  |  |  |
| 1 | X |  |  |  |  |  |  |  |
| 2 | X |  |  |  |  |  |  |  |
| 3 | X |  |  |  |  |  |  |  |
| 4 | X |  |  |  |  |  |  |  |
| 5 | X |  |  |  |  |  |  |  |
| 6 | X |  |  |  |  |  |  |  |
| 7 | X |  |  |  |  |  |  |  |
| 8 | X |  |  |  |  |  |  |  |
| 9 | X |  |  |  |  |  |  |  |
| 10 | X |  |  |  |  |  |  |  |
| 11 | X |  |  |  |  |  |  |  |
| 12 | X |  |  |  |  |  |  |  |
| 13 | X |  |  |  |  |  |  |  |
| 14 | X |  |  |  |  |  |  |  |
| 15 | X |  |  |  |  |  |  |  |
| 16 | X |  |  |  |  |  |  |  |
| 17 | X |  |  |  |  |  |  |  |
| 18 | X |  |  |  |  |  |  |  |
| 19 |  | X |  |  |  |  |  |  |
| 20 |  | X |  |  |  |  |  |  |
| 21 | X |  |  |  |  |  |  |  |
| 22 | X |  |  |  |  |  |  |  |
| 23 | X |  |  |  |  |  |  |  |
| 24 | X |  |  |  |  |  |  |  |
| 25 | X |  |  |  |  |  |  |  |
| 26 |  | X |  |  |  |  |  |  |

## 6.1 Solution #1: Inverse AKA

### 6.1.1 Introduction

This solution addresses the Key Issue #1 and applies for S&F operations in EPS and 5G.

### 6.1.2 Solution details

This solution, by reversing roles between UE/USIM and network, enables an Authentication and Key Agreement mutual scheme, with same security level as the usual one.

Those reversed roles, because UE is originating the procedure, enable to cope with the connection discontinuity introduced by intermittent satellite coverage. UE generating AV can directly secure the user data to be attached as payload associated with first signalling messages.

This solution also enables to optimize the satellite communication by including user data attached to signalling NAS message during attachment, maintaining, at each step the security level.

#### 6.1.2.1 Solution details for S&F in EPS

The main steps of this solution in EPS are the following:



Figure 6.1.2.1-1 : Inverse AKA and data exchange in EPS

If the UE has data to send uplink, when it detects the satellite in S&F mode, the steps are the following:

1. (Optional step) UE and satellite setup a secure channel in order to mutually authenticate each other.
2. The UE creates a 4G AV. The UE does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1". The UE shall then calculate XRES as defined in TS 33.401 [3] and create an AV from RAND, AUTN, XRES.
3. The UE shall then derive keys from CK, IK as defined in EPS key hierarchy of TS 33.401 [3]
4. UE encrypts payload: UL user data with NAS keys
5. UE sends ATTACH REQUEST containing RAND, AUTN, XRES and UL data as encrypted payload on service link
6. Satellite stores information…
7. …till it will be able to reopen a feeder link with ground network
8. Thanks to feeder link now available, satellite sends ATTACH REQUEST containing RAND, AUTN, XRES and UL data as encrypted payload to MME.
9. MME stores XRES and encrypted UL user data message.
10. MME sends AUTHENTICATION REQUEST to HSS/AuC together with IMSI/GUTI, RAND and AUTN
11. HSS/AuC verifies AUTN. To avoid any synchronization issue, it will be recommended to use time-based SQN generation.
12. If OK, HSS/AuC computes RES, CK, IK and generates KASME
13. HSS/AuC sends AUTHENTICATION RESPONSE to MME with RES and KASME
14. MME compares XRES with RES and if OK generates keys from KASME as defined in EPS key hierarchy of TS 33.401[3]
15. MME can decrypt UL data with NAS keys
16. If data are to be sent Down Link, MME encrypts DL data with NAS keys
17. MME sends RRC security mode command to eNodeB to provide RRC keys.
18. MME sends ATTACH COMPLETE message with RES and encrypted DL data as payload.
19. If service link is not available, satellite/eNodeB store the NAS message.
20. eNodeB proceeds to RRC key derivation.
21. When service link becomes available, both endpoints know RRC keys.
22. when service link becomes available …
23. eNodeB forwards the ATTACH COMPLETE message with RES and encrypted DL data as payload message to the UE.
24. UE verifies the RES.
25. The UE processes the potential encrypted DL data as payload message to the UE

Editor's Note: The negotiation of security algorithm use for NAS security is FFS.

#### 6.1.2.2 Solution details for S&F in 5G

The main steps of this solution in 5G are the following:



Figure 6.1.2.2-1: Inverse AKA and data exchange in 5G

1. Optional step. UE and satellite setup a secure channel to mutually authenticate each other.

2. The UE creates a 5G AV. The UE does this by generating an AV with the Authentication Management Field (AMF) separation bit set to "1" as defined in TS 33.102 [7]. The UE then calculates XRES\* as defined in TS 33.501 [4] and creates a 5G AV from RAND, AUTN, HXRES\*. Finally, the UE generates a SUCI as defined in TS 33.501 [4].

3. The UE then derives keys from CK, IK as defined in TS 33.501 [4] till User Plane keys and generates UL user data protected by NAS keys.

NOTE: The negotiation of security algorithm used for NAS security could be done in different manners: e.g. the USIM could be configured with algorithms to use, or negotiation messages could be exchanged between the UE and the satellite before step 2.

4. The UE uses service link to send to the satellite the REGISTRATION REQUEST for the SUCI with 5G AV and first UL data, as encrypted payload

5. Satellite stores all those information…

6. …till it will be able to reopen a feeder link with ground network

7. Thanks to feeder link now available, satellite sends that information to AMF/SEAF

8. AMF/SEAF stores HXRES\* and first user data message

9. AMF/SEAF sends SUCI, RAND and AUTN to AUSF

10. AUSF sends them to UDM/ARPF as part of authentication request

11. UDM invokes SIDF to de-conceal the SUCI

12. Based on K and RAND, the UDM/ARPF verifies the freshness of the received values by checking whether AUTN can be accepted (MAC-A, SQN).

13. The UDM/ARPF computes RES, CK, IK and then computes RES\* and KAUSF

14. The UDM/ARPF return SUPI, RES\* and KAUSF to the AUSF

15. The AUSF generates KSEAF from KAUSF

16. The AUSF sends to AMF/SEAF, RES\*, SUPI and KSEAF

17. The AMF/SEAF generates HRES\* from RES\* and compare it to previously received HXRES\*

18. The AMF/SEAF processes the first user data message previously received

19. The AMF/SEAF processes the potential user data DL message for the UE

20. The AMF/SEAF determine the next satellite over the zone and send key material for RRC protection

21. The AMF/SEAF send to the satellite the REGISTRATION ACCEPT with RES\* and user data DL message if any as encrypted payload.

21. Satellite stores all those information…

22. …till it will be able to reopen a service link with UE, RRC protected

23/24. The satellite sends to UE, the REGISTRATION ACCEPT with RES\* and user data DL message if any as encrypted payload.

25. The UE verifies the RES\*

26. The UE processes the potential user data response message

### 6.1.3 Evaluation

This solution addresses the Key Issue #1 and applies for S&F operations in EPS and 5G.

This solution fulfills the potential security requirements from the Key Issue #1.

This solution, by reversing roles between UE/USIM and network, enables an Authentication and Key Agreement mutual scheme, with same security level as the usual one.

Those reversed roles, because UE is originating the procedure, enable to cope with the connection discontinuity introduced by intermittent satellite coverage. UE generating AV can directly secure the user data to be attached as payload associated with first signalling messages.

This solution also enables to optimize the satellite communication by including user data attached to signalling NAS message during attachment, maintaining, at each step the security level. The optimization is due to reduced number of store and forward phases to exchange data between the UE and the ground compared to usual AKA procedure.

This solution has impacts on the ME, USIM, MME/AMF/SEAF, HSS/AuC/UDM/AUSF/ARPF.

There is a low risk of indirect DoS attack on HSS or AUSF/UDM in case that the UEs are injective many AVs (in loop or random) towards the satellite since the solution proposes to optionally setup a secure channel between the UE and the satellite to ensure that only authenticated and authorized UEs can communicate with the satellite to perform inverse AKA procedure. Additionally, in solution for EPS, if the satellite has received several AVs, then the satellite proceeds only the last received AV.

## 6.2 Solution #2: IOPS security concept for S&F

### 6.2.1 Introduction

This solution addresses the Key Issue #1 and applies for S&F operations in EPS and 5G.

### 6.2.2 Solution details

To provide registration capabilities if feeder link is not available, this solution proposes to have HSS/AuC (resp. AUSF/UDM/ARPF/SIDF) capabilities on board the satellite to run the classical AKA procedure. But HSS/AuC (resp. AUSF/UDM/ARPF/SIDF) contains subscriber key credentials and there is a security risk to have such credentials on board the satellite, for example if satellite is lost or stolen, the user subscription credentials might be compromised.

To mitigate this risk, this solution considers the satellite in Store and forward mode re-using security architecture and principals as described in TS 33.401 [3] Annex F “Isolated E-UTRAN Operation for Public Safety”.

#### 6.2.2.1 Solution details for S&F in EPS

For 4G system, this solution implies that the satellite acts as local EPC including at least MME and HSS functionality, and that, following IOPS security concept, the HSS/AuC on board the satellite only contains derived keys from master key MK, for the given the satellite.

Compared to classical 4G AKA, the UE first retrieves E-UTRAN Cell Identity and provides it to the USIM, that will derive the subscriber master key to obtain symmetrical key K\_nsat for this satellite. Nominal AKA procedure will be performed after with symmetrical key K\_nsat.

The main steps of this solution in EPS are the following:



Figure 6.2.2.1-1: IOPS security concept applied to S&F in EPS

Initial conditions:

- USIM is configured with IMSI and master key MK for local PLMN

- HSS/AuC on board of the satellite is configured with IMSI and derived key K\_nsat for satellite Nsat.

- Satellite identifier nsat matches eNodeB\_Id.

1. UE detects service link and selects the local PLMN.

2. UE sends ATTACH request to the local MME

3. Local MME generates the AUTHENTICATE REQ to the local HSS/AuC for the requesting IMSI

4. Local HSS/Auc generates AV from the key Knsat derived from MK for the satellite nsat. Proprietary bit of AMF is used to indicate that the authentication is performed with a satellite acting as a local network

5. Local HSS returns authentication response to the local MME

6. Local MME challenges the UE with RAND and AUTN

7. ME challenges the USIM, with RAND, and AUTN with proprietary bit of AMF to indicate that the authentication is performed with a satellite acting as a local network for the AUTHENTICATE CMD. The ECI (E-UTRAN Cell Id) is also added as parameter to the command for the USIM to perform the derivation.

8. USIM retrieves nsat from ECI

9. Derivation of K\_nsat from MK by the USIM. The USIM checks AMF value and derives K\_nsat from MK thanks to KDF where n=nsat stored previously. The derived key K\_nsat takes the role of permanent subscriber K to perform AKA procedure

10. USIM returns RES and keys computed with this K\_nsat

11. Normal continuation of the ATTACH procedure

#### 6.2.2.2 Solution details for S&F in 5G

For 5G system, this solution implies that the satellite acts as local 5GC including at least AMF and AUSF/UDM/ARPF/SIDF functionalities. The concept described in Annex F of TS 33.401 [3] is reused, where ECI is replaced by NR Cell Global Id (NCGI) and the SUPI/SUCI (de)concealment steps are added.

The main steps of this solution in 5G are the following:



Figure 6.2.2.2-1: IOPS security concept applied to S&F in 5G

Initial conditions:

* USIM is configured with SUPI and master key MK for local PLMN, together with master key and certificate for SUPI/SUCI: Master Key SUCI\_MK, Master SUCI PK QM
* Local AUSF/UDM/ARPF/SIDF on board of the satellite is configured with SUPI and derived key K\_nsat for satellite nsat, together with private key for SUCI.
* Satellite identifier nsat matches gNodeB\_Id.

1. UE detects service link and select the local PLMN.
2. GET IDENTITY COMMAND with specific context to provide NCGI (NR Cell Global Identifier) as parameter.
3. USIM retrieves nsat from NCGI. NCGI value is different for each satellite.
4. USIM derives SUCI Public Key for “nsat”. The derived Public Key can be stored in the USIM for future use.
5. USIM computes SUCI.
6. USIM responds with SUCI.
7. UE sends REGISTRATION REQUEST request to the local AMF.
8. Local AMF generates the AUTHENTICATE REQ to the local AUSF/UDM/ARPF/SIDF for the requesting SUCI.
9. local AUSF/UDM/ARPF/SIDF de-conceals the SUCI.
10. Local AUSF/UDM/ARPF/SIDF generates AV from the key K\_nsat derived for the satellite nsat. Proprietary bit of AMF is used to indicate that the authentication is performed with a satellite acting as a local network
11. Local AUSF/UDM/ARPF/SIDF returns authentication response to the local AMF.
12. Local AMF challenges the UE with RAND and AUTN.
13. UE challenges the USIM with RAND, and AUTN with proprietary bit of AMF to indicate that the authentication is performed with a satellite acting as a local network for the AUTHENTICATE CMD.
14. Derivation of K\_nsat from MK by the USIM. The USIM checks AMF value and derives K\_nsat from MK thanks to KDF where n=nsat stored previously. The derived key K\_nsat takes the role of permanent subscriber key to perform AKA procedure.
15. USIM returns RES and keys computed with this K\_nsat.
16. Normal continuation of the REGISTRATION procedure.

### 6.2.3 Evaluation

This solution addresses the Key Issue #1 and applies for S&F operations in EPS and 5G.

This solution fulfils the potential security requirements from the Key Issue #1.

The master key associated with the subscription is not compromised in any case. On the UE side, the subscriber master MK is securely stored in USIM.

This solution has impacts on the ME, USIM, HSS/AuC/UDM/AUSF/ARPF.

Editor's Note: The performance impacts on HSS/UDM processing, authentication latency, and service-link capacity are FFS.

Editor's Note: It is FFS whether the solution can support roaming scenarios.

Editor's Note: Further evaluation is FFS.

## 6.3 Solution #3: IOPs based solution for UE to satellite security

### 6.3.1 Introduction

This solution addresses key issues #1 and #2.

It applies to an architecture when a complete network is deployed in the satellite or set of interlinked satellites..

### 6.3.2 Solution details

This solution applies to the case that the whole network, i.e. serving and home network, is hosted in the satellite or set of satellites. For EPS this includes deploying an HSS in the (set of) satellite(s). In this case all the security procedures that are used between the UE and satellite(s) are the same one as used between the UE and network in regular 3GPP access.

Such a type of solution requires the pre-configuration of credentials that are used to authenticate with the UE in the satellite. In order to enable different keys to be configured in different satellites for the same UE, it is proposed to use a solution like the one described in Annex F.4 of TS 33.401 [3].

NOTE: As all the parameters used in Annex F.4 of TS 33.401 [3] relate to the authentication between the UE and network and are in effect under an operator’s control, solution similar to one described could be used.

The solution described in Annex F.4 of TS 33.401 [3] uses bits of the AMF field in the AUTN parameter and also possibly the IND part of the sequence number SQN, as described in Annex C.1 of TS 33.102 [7] to calculate a root key for the authentication between the UE and particular (set of) satellite(s). This means that a different key can be used between the UE and each different (set of) satellite(s). This is achieved using existing information and hence requires no update to the signalling that is used between UE and regular networks.

The solution supports roaming by having the relevant key for the UE provisioned into the satellite PMLN’s HSS (which does not have to be the UE’s HPLMN). Provisioning such a key enables the UE to access the PLMN supported by the satellite.

With this solution, there is only a need to re-establish the security when the UE moves away from the set of interlinked satellites and the overall processing in the HSS in authenticating a UE is the same regardless of the location of the HSS. The authentication latency is small and the reliability is high with the HSS in the satellite(s) as it is always possible to authenticate the UE in a single uninterrupted operation.

### 6.3.3 Evaluation

TBD

## 6.4 Solution #4: Store and forward satellite operation

### 6.4.1 Introduction

This solution addresses “Key issue #1: Security protection in Store and Forward Satellite Operation”.

In the solution it is assumed that the normal 5GC registration procedure is not able to be performed due to time outs of the different protocols. It is proposed here that the UE and the 5GC perform a provisional one-round-trip procedure for a provisional registration, i.e. the UE is not fully registered at this point in time, thus is not e.g. eligible to receive terminating data or establish a PDU session. The UE and the network may generate a provisional key for the NAS signalling only valid for one small data transmission, the UE and satellite may use also a provisional key for the RRC signalling. The UE receives a token from the 5GC to compute a result from the challenge to authenticate itself when it sends the small data in a NAS message, which may be protected by a provisional key. The provisional NAS key will be derived without NAS SMC procedure in order to save one round trip of messages. The network may assign a new token in the acknowledgement of the NAS message for the next time usage.

In that way, the small data is protected via the store and forward network and, depending on the validity time of the token, it is not time sensitive that a procedure needs to be carried out within a specific time window. The small data is transferred within the NAS message similar to the small data IoT feature. Each time the UE sends small data, it derives the new NAS keys and computes the corresponding authentication result from the previously received token.

The solution is split into two parts, the provisional registration procedure and the small data transmission within a NAS message, including the authentication response token.

The key features of the solution are the following:

Solution is independent of the specific system link which is not available. Interruption of the logical RRC and NAS connections are mitigated by this solution.

A key feature of this solution is bundling the authentication round trip with the NAS SMC in one message. The authentication token the normal auth challenge in 5G-AKA or EAP-AKA’ using preconfigure default values e.g. for UL Count so that both sides can derive the whole set of keys without waiting for the UE to reply.

Authorization for a UE to use this solution can be achieved via checking in the AUSF when generating the authentication challenge, or in the UDM when de-concealing the SUCI.

Solution depends on an indication that a satellite supports Store-and-Forward operation, e.g., via a future T.B.D. SIB message.

Solution may be used to mitigate connectivity interruptions due to outages of the inter satellite links and/or feeder links when a UE has small messages to send, e.g. when a UE is operating in MICO mode.

### 6.4.2 Solution details



Figure 6.4.2-1: Provisional Registration Procedure

1. The UE sends a NAS Registration Request to the store and forward satellite network. The UE includes an indication for the AMF that the registration is via store and forward and not a normal registration procedure. The NAS timer for this Registration message is much longer than usual for normal registrations to ensure the timer does not expire until the response message it received later.

2. The satellite stores the NAS message and forwards it to the AMF once the link becomes available.

3. The AMF/SEAF sends an Nausf\_UEAuthentication\_Authenticate Request message to the AUSF including the indication that the registration is via store and forward network. The indication helps AUSF not to let the registration procedure time out and to keep the UE in a provisional registration state after sending out the authentication challenge and to derive already the NAS keys without NAS SMC.

4. The AUSF sends the Nudm\_UEAuthentication\_Get Request to the UDM including the indication that the registration is via store and forward network.

5. The UDM selects the authentication mode and creates an authentication token for the UE, i.e. the authentication token has the form of the authentication challenge of EAP-AKA’ or 5G-AKA that can be computed by the UE to an expected result in a similar way as in the UDM. The UDM derives the key KAUSF based on the selected authentication token and computes an expected authentication result.

6. The UDM sends an Nudm\_UEAuthentication\_Get Response to the AUSF, including the authentication token and the authentication result.

7. The AUSF marks the UE as provisional authentication based on the indication that the registration is via store and forward network and the authentication token. The AUSF derives the KSEAF from the KAUSF.

8. The AUSF sends a Nausf\_UEAuthentication\_Authenticate Response to the AMF including the authentication token and KSEAF. This is different from existing procedure where KSEAF is provided only upon receiving authentication success message from the UE.

9. The AMF derives both the KAMF and the provisional NAS keys from KSEAF without performing a NAS SMC procedure. The default algorithms for integrity and confidentiality maybe preconfigured in the AMF and UE. The UE is marked in the AMF as provisionally registered, i.e. the UE can send small data in the protected NAS messages but cannot receive any terminating services since it does not have a PDU Session and would not get paged by the AMF.

10. The AMF sends a Registration Accept to the UE via the store and forward satellite including an indication that the registration is provisional and the authentication token.

11. The serving satellite sends a Registration Accept to the UE including an indication that the registration is provisional and the authentication token.

12. The UE computes the authentication result from the authentication token. It computes the keys in the same way as the 5GC including the provisional NAS keys from the long term key K with the same default configuration. The NAS keys are then used to confidentiality and integrity protect the NAS message sent via the store and forward links including the embedded small data.

The next figure describes the transmission of the small data packet within the protected NAS message:



Figure 6.4.2-2: Protected Small Data Transmission

1. The UE sends a NAS Request to the store and forward satellite network. The UE includes its identifier, the authentication result, computed from the previously received authentication token, and the small data. The NAS message is confidentiality and integrity protected with the provisional NAS keys. The NAS timer for the NAS message is much longer than usual for normal messages to ensure the timer does not expire until the response message it received later.

2. The satellite stores the NAS message and forwards it to the AMF once the link becomes available.

3. The AMF/SEAF sends an Nausf\_UEAuthentication\_Authenticate Request message to the AUSF including the authentication result.

4. The AUSF verifies the received authentication result with the one received from the UDM in the provisional registration procedure. If the verification is successful, the AUSF keeps the UE as provisional authenticated and requests a fresh authentication token from the UDM.

5. The AUSF sends the Nudm\_UEAuthentication\_Get Request to the UDM including the indication that the registration is via store and forward network to request a new authentication token. The AUSF may include the verification result.

6. The UDM selects the authentication mode and creates a new authentication token for the UE, i.e. the authentication token has the form of the authentication challenge of EAP-AKA’ or 5G-AKA that can be computed by the UE to an expected result in a similar way as in the UDM. The UDM derives the new key KAUSF based on the selected authentication token and computes an expected authentication result.

7. The UDM sends an Nudm\_UEAuthentication\_Get Response to the AUSF, including the new authentication token and the new authentication result.

8. The AUSF keeps marking the UE as provisional authentication based on the indication that the registration is via store and forward network and the new authentication token. The AUSF derives the new KSEAF from the KAUSF.

9. The AUSF sends a Nausf\_UEAuthentication\_Authenticate Response to the AMF including the new authentication token and the verification result.

10. The AMF forwards the small data to the respective network function if the verification result is successful. The AMF derives the new KAMF and the new provisional NAS keys without performing a NAS SMC procedure. The default algorithms for integrity and confidentiality maybe preconfigured in the AMF and UE. The UE is kept marked in the AMF as provisionally registered, i.e. the UE can send small data in the protected NAS messages but cannot receive any terminating services since it does not have a PDU Session and would not get paged by the AMF.

11. The AMF sends a NAS Response message to the UE protected with the old provisional NAS keys via the store and forward satellite including an acknowledgement for the small data and the new authentication token. The AMF may delete the old NAS keys after the protection of this message, also considering the NAS retransmission timers.

12. The serving satellite sends a NAS Response message to the UE including an acknowledgement for the small data and the new authentication token.

13. The UE computes the new authentication result from the new authentication token. It computes the new keys in the same way as the 5GC including the provisional NAS keys from the long term key K with the same default configuration. The new NAS keys are then used to confidentiality and integrity protect the next NAS message sent via the store and forward links including the embedded small data. The UE may delete the old NAS keys after the successful reception of the NAS Response message.

### 6.4.3 Evaluation

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

Solution is independent of the specific system link which is not available. Interruption of the logical RRC and NAS connections are mitigated by this solution.

A key feature of this solution is bundling the authentication round trip with the NAS SMC in one message. The authentication token the normal auth challenge in 5G-AKA or EAP-AKA’ using preconfigure default values e.g. for UL Count so that both sides can derive the whole set of keys without waiting for the UE to reply.

Authorization for a UE to use this solution can be achieved via checking in the AUSF when generating the authentication challenge, or in the UDM when de-concealing the SUCI.

Solution depends on an indication that a satellite supports Store-and-Forward operation, e.g., via a future T.B.D. SIB message.

Solution may be used to mitigate connectivity interruptions due to outages of the inter satellite links and/or feeder links when a UE has small messages to send, e.g. when a UE is operating in MICO mode.

## 6.5 Solution #5: Onboard UDM

### 6.5.1 Introduction

This solution addresses key issue #1.

During the feeder link’s intermittent unavailability, in order for the completion of authentication and NAS security procedures, UDM/AUSF could be onboard.

### 6.5.2 Solution details

The following assumptions and principles apply:

- The gNB, AMF and UDM/AUSF are placed on board the same satellite.

- The UE has a subscription and credentials in the onboard UDM. The long term key onboard is the same as the one on the ground.

- The onboard UDM is synchronized with the UDM on the ground when feeder link is available.



UE



SMF

UPF

AMF



RAN

UPF

DN

UDM/AUSF

Figure 6.5.2-1:

When the gNB, AMF and UDM/AUSF are all on board, the authentication and NAS security procedures follow what defined in TS 33.501[4]. The differences are:

- After the on-board registration completion, the on-board UDM may send the authentication result to the ground UDM for backup.

Editor’s Note: It is FFS whether the solution can support roaming scenarios.

Editor’s Note: If UE is served by single satellite hosted 3GPP systems or multiple is FFS.

Editor’s Note: How does onboard UDM sync with ground UDM is FFS.

### 6.5.3 Evaluation

TBD

Subscriber credentials are provisioned in several satellites UDMs. If one of the satellites is compromised by an attacker, either in the form that the attacker could obtain the subscriber credentials or that the attacker could control the interface to the UDM of the satellite, and if, for any given subscriber, the credentials in the UDM of the satellite were the same, this would imply that, for all subscribers whose credentials were stored in the compromised satellite, the subscriber credentials would have to be re-provisioned in the USIMs in the field and all satellites UDMs.

The key used to generate authentication vectors should be stored on the satellite, which may not be the resources of the home operator.

## 6.6 Solution #6: Primary authentication and NAS security context establishment during store-and-forward operations

### 6.6.1 Introduction

This solution proposes the following:

* Including Satellite Access Type information in Initial UE message from Satellite gNB to AMF, to allow serving network AMF know about possible intermittent loss of feeder link communications.
* Updating NAS timers (e.g. T3510, T3511) to enable primary authentication and NAS security context establishment with UEs during store-and-forward operations as per legacy procedures.

### 6.6.2 Solution details



Figure 6.6.2-1: Message flow for security procedures between UE and NAS with S&F operations

Figure 6.6.2-1 shows the message flow for secure primary authentication and NAS security context establishment in S&F operations. In this solution:

* The delays incurred due to intermittent loss of feeder link connectivity can be minimized by using ISLs to make the NAS Registration Request message reach the ground network. However, since SA2 assumes that Store and Forward Satellite Operation shall work without ISL, this optimization is not considered in this solution.
* If timer T3510 expires at AMF or at UE, a new Reject cause is proposed which indicates that the rejection is due to delays in S&F operations. Also, the reject message with this new cause includes updated NAS timers for S&F operations.
  + Updated values of NAS timers can be computed, for e.g., by observing the time between first and second attempts of NAS Registration Request from UE.
  + Also, the satellite which does not have feeder link connectivity when it receives the RRC Connection Setup Complete can provide an estimate of the time needed for the round-trip communications between itself and core network for primary authentication and NAS Registration procedures.
* If the NAS timers for S&F operations are pre-computed, SoR or UPU or OTA methods maybe used to update the NAS timers in UEs which connect via the satellite access.
* As the Satellites are moving, it is likely that timer values vary for different UEs in the same coverage area. Considering this fact, the AMF can store the computed value and statistically calculate more accurate NAS timers for SAT access.
* In multi-satellite scenarios, especially considering LEO satellites which may move out between two consecutive NAS registration attempts from the UEs, AMF and core network can independently compute the required NAS timer values for satellite access type using information about satellite movements, as well as statistically analysing the time between two consecutive NAS registration attempts received by the core network from the same UE.
  + NOTE: This solution focuses on the timers associated with UE authentication and NAS registration procedures and does not consider handovers between satellites (when UEs are in RRC Connected mode).

### 6.6.3 Evaluation

Impacted entities: UE, RAN and AMF

This solution enables re-use of legacy procedures for UE authentication and NAS security context establishments with satellite access type in store-and-forward operations by adapting NAS timers according to the delays observed between the UEs and the core network.

Editor’s Note: Further evaluation is FFS.

Editor’s Note: Impact of unprotected reject message is FFS.

## 6.7 Solution #7: Optimization of subsequent authentication procedure in S&F operation

### 6.7.1 Introduction

This solution addresses the security requirement of key issue#1. The solution assumes that atleast gNB and AMF are on-board on satellite. This solution is only applicable for subsequent authentication procedure.

### 6.7.2 Solution details

#### 6.7.2.1 Provisioning of authentication vectors



Figure 6.7.2.1-1: Provisioning of Authentication Vectors for subsequent authentications

1. The UE and the 5G CN performs the Initial Registration procedure and NAS security context exists between the UE and AMF when the service link is available. The identifier of the serving AMF serving the UE in the access through which the UE has registered is registered in the UDM.
2. Upon receiving the request from the AMF, based on the TAI received in Nudm\_UECM\_Registration the UDM/ARPF generates a set of authentication vectors as defined in TS 33.102 [7].
3. Upon generating AVs, the UDM sends the list of AVs to the AUSF.
4. Upon receiving the list of 5G HE AVs and SUPI, the AUSF stores list of 5G HE AVs and the corresponding SUPI.
5. Further the AUSF performs the protection of AUTNs and RANDs (as like in SoR or UPU procedure) and send it to the UDM. The UDM performs the UE Parameters Update (UPU) using the control plane procedure while the UE is registered to the 5G system as detailed in 6.15.2.1 of TS 33.501 [4] and provides the list of RANDs and AUTNs to the UE. Upon receiving the list of RANDs and AUTNs, the UE verifies the received AUTNs and calculate the RES and stores it.

#### 6.7.2.2 Optimized subsequent authentication procedure



Figure 6.7.2.2-1: Optimized subsequent authentication method

1. In a N1 message to the UE, the SEAF includes the authentication request indication and the ciphering and the integrity algorithm. Authentication request indication is to indicate the UE to perform authentication when performing next NAS procedure (i.e., Registration or PDU session establishment).
2. When initiating a NAS procedure, the UE selects an unused SQN/AUTN and corresponding RAND from the stored values.
3. UE derives the RES\* from the selected AUTN and RAND, if not derived when storing the received AUTN and RAND.

Based on the keys derived from the selected AUTN/SQN and RAND and the network indicated integrity algorithm (non-current 5G security context), the UE derives the MAC-I on the N1 request message.

1. The UE then sends an N1 message request to the SEAF. The message includes the SUCI or 5G-GUTI, RES\*, RAND, SQN and NAS MAC-I. The NAS MAC-I is used for integrity protection of the message.
2. Upon receiving the N1 message request from the UE, the SEAF stores the NAS MAC-I for the later integrity check.
3. The SEAF invokes the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the SEAF wants to initiate an authentication. This message includes SUCI or SUPI, SN-name, RAND, SQN and RES\*.
4. Upon receiving the Nausf\_UEAuthentication\_Authenticate Request message, the AUSF sends Nudm\_UEAuthentication\_Get Request to the UDM, if there is no 5G HE AV available with the AUSF for the SUPI. If the AUSF able to retrieve the 5G HE AV for the received SUPI, RAND and SQN, then the AUSF performs the step 10, (skipping steps 6, 7, 8 and 9).

The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;

- the serving network name;

- RAND and SQN

1. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM invokes SIDF if a SUCI is received. SIDF de-conceals SUCI to gain SUPI before UDM can process the request.
2. The UDM/ARPF generates the authentication vectors for the received RAND and SQN and the SUPI.
3. The UDM subsequently sends the 5G HE AV to the AUSF using a Nudm\_UEAuthentication\_Get Response message.
4. The AUSF compared the XRES\* with the RES\* received from the SEAF in the Nausf\_UEAuthentication\_Authenticate Request message.
5. The AUSF then generates the 5G AV from the 5G HE AV received from the UDM/ARPF by computing the HXRES\* from XRES\* (according to Annex A.5 of TS 33.501[4]) and KSEAF from KAUSF (according to Annex A.6 of TS 33.501), and replacing the XRES\* with the HXRES\* and KAUSF with KSEAF in the 5G HE AV.
6. The AUSF indicates to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response whether the authentication was successful or not from the home network point of view. If the authentication was successful, the KSEAF is sent to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response. The AUSF also includes the 5G SE AV (RAND, AUTN, HXRES\*) in the response message. In case the AUSF received a SUCI from the SEAF in the authentication request, and if the authentication was successful, then the AUSF also includes the SUPI in the Nausf\_UEAuthentication\_Authenticate Response message.
7. The SEAF then computes HRES\* from RES\* according to TS 33.501[4], and the SEAF compares HRES\* and HXRES\*. If successful, the SEAF considers the authentication successful from the serving network point of view. The SEAF derives further keys to establish the NAS security context.
8. The SEAF verifies NAS MAC-I received in Step 3 with the NAS MAC-I calculated at the network side, using the derived NAS security context.
9. Once the verification is successful, the SEAF starts Integrity protection, uplink deciphering and downlink ciphering.
10. The SEAF sends the N1 message to the UE. This message includes ngKSI (either generated or the received ngKSI from the UE), UE security capabilities and NAS MAC-I.
11. Upon receiving the N1 message from the SEAF, the UE verifies the NAS message integrity and if successful, it starts the uplink ciphering and the downlink deciphering (i.e., UE makes the non-current 5G security context to current 5G security context).

NOTE: It is out-of-scope of this solution to address the DoS attack mounted by the malicious UEs with valid subscription.

### 6.7.3 Evaluation

This solution addresses the first and second requirements of key issue#1.

This solution mostly follows inverse AKA procedure but is applicable only for subsequent authentication. The solution requires the UE to be provisioned with the required one or more AVs to be utilized during subsequent authentication.

## 6.8 Solution #8: Solution on preventing DoS attacks in S&F operation

### 6.8.1 Introduction

This solution addresses key issue #1: Security protection in Store and Forward Satellite Operation.

When only service link is available, a satellite may receive a number of registration request messages from UEs which are not authenticated yet. Unless there is a means for the satellite to verify whether the messages are from valid UEs or not, the satellite would store and forward all of the received messages. It may lead to a DoS (denial of service) attack on the satellite.

In addition, after a valid UE sends registration request message, the UE will wait till the service link is available again for authentication. However, if the satellite is a false satellite, the UE may not be able to connect to core network for a long time. It may lead to a DoS attack on the UE. The DoS attacks described above may happen more easily than a ground base station case, due to the Store and Forward property.

In this solution, before the primary authentication is performed between the UE and core network, ECCSI (elliptic curve-based certificateless signatures for identity-based encryption) as defined in IETF RFC 6507 [8] is used for mutual authentication between UE and satellite, in order to prevent the DoS attacks. In this solution, it is assumed that a satellite includes eNB and the functionality of MME related to the authentication called MME (NT).

### 6.8.2 Solution details



Figure 6.8.2-1: Protected attach procedure with MME onboard the satellite in S&F operation

To prevent DoS attacks, the following procedure is preceded:

1. The network provisions UEs and Satellite with a set of credentials for ECCSI. The credentials include Public Validation Token (PVT), Secret Signing Key (SSK) associated with UE's or Satellite's identity, and KMS Public Authentication Key (KPAK).

NOTE: KMS can be a standalone entity or collocared in an existing NF.

After that, the authentication process of S&F mode is as follows.

PHASE 1. (Service link is available, Feeder link is unavailable)

1. The satellite provides a random number generated by the satellite (SAT.RN) and S&F indicator indicating that the satellite is operating in S&F mode. These may be included in the SIB (System Information Broadcast) message
2. The UE initiates the attach procedure by transmitting signed Attach Request message. This message consists of the Attach Request message (UE.ID, UE.RN, SAT.RN, and S&F indicator in addition to existing parameters) and digital signature. UE.ID of the message, generated by the UE through ECCSI. UE.ID is the UE's identity associated with ECCSI algorithm, and S&F indicator indicates that the UE will operate in S&F mode.

The satellite checks the validity of the UE by verifying the UE.Sig.

1. If the verification is successful, the satellite stores the received attach request message and transmits signed Attach Reject message. This message consists of the Attach Reject message (SAT.ID, and Re-attach Info) and digital signature which is generated by the satellite using the Attach Reject message and UE.RN through ECCSI algorithm. SAT.ID is the satellite's identity associated with ECCSI algorithm and the Re-attach Info is information necessary for the UE to attempt the reconnection in step 7 (e.g., information about when the UE should retry to reconnect or list of satellite(s) that the UE should retry to reconnect).

The UE checks the validity of the satellite by verifying the SAT.Sig. If verified, UE waits for step 7 based on the guideline received.

PHASE 2. (Service link is unavailable, Feeder link is available)

1. The satellite requests authentication data for the UE by sending the Authentication Data Request message to the ground network (GND). The request includes IMSI, SN identity, and Network type.
2. Upon the receipt of the Authentication Data Request from the satellite, HSS in the GND generates Authentication Vector(s) as defined in clause 6.3.2 in TS 33.102 [7]. Authentication Vector consists of KASME, RAND, AUTN, and XRES.
3. The GND sends an authentication response back to the satellite that contains Authentication Vector(s).

PHASE 3. (Service link is available, Feeder link is unavailable)

The satellite in this PHASE may be different from the satellite in PHASE 1.

1. The UE retries the network connection by transmitting the Attach Request.

Editor's Note: Whether step 7 needs to be protected is FFS.

1. The satellite sends Authentication Request including AUTN and RAND.
2. At the receipt of the RAND and AUTN, the UE verifies the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102 [7]. If so, the UE computes a response RES.
3. UE responds with Authentication Response message including RES in case of successful AUTN verification. In this case, the UE computes KASME from CK, IK, and serving network's identity.
4. The satellite checks that the RES equals XRES. If so, the authentication is successful. As a result of the authentication and key agreement, an intermediate key KASME is shared between the UE and the satellite.
5. NAS SMC procedure is performed between the UE and the satellite.

Editor’s Note: System impact is FFS.

NOTE: The dynamic variation of SAT.RN and UE.RN hardens the security against DoS.

### 6.8.3 Evaluation

This solution satisfies all of the potential security requirements in KI#1.

In particular, before the AKA procedure between the UE and the network is completed, the satellite and the UE check the authenticity of each other using the asymmetric cryptosystem (i.e., ECCSI), which prevents the threat of DoS attack related to storage issue in the satellite. However it does not address the DoS attack on resources such as processing and memory consumpution in the satellite.

To achieve this, the following changes are needed:

* eNB on a satellite generates and verifies a digital signature.
* UE generates and verifies a digital signature.

Therefore, this solution might require slightly more computational resource, but it will eliminate waste of storage resource of a satellite, which causes DoS attack captured in KI#1.

In addition, this solution further prevents the attacks from a fake satellite, which are the threats already captured in some solutions from TR 23.700-29 [2].

Editor's Note: Further evaluation is FFS.

## 6.9 Solution #9: Secure Initial Registration for S&F satellite operation

### 6.9.1 Introduction

This solution specifically addresses the security considerations of Key Issue #1, which pertains to supporting Store and Forward Satellite operations. The Initial Attach / Initial Registration process is crucial for all S&F services. It must ensure the network's integrity and security despite the unique challenges posed by satellite communication, such as intermittent connectivity.

### 6.9.2 Solution details

Considering a scenario with a single Low-Earth Orbit (LEO) satellite providing intermittent coverage, this solution proposes modified MME functionality: one segment aboard the satellite (MME-SAT) and the other on the ground (MME-GND). This split architecture accommodates satellite coverage's intermittent connectivity and facilitates secure communication between the UE and the network.



Figure 6.9.2-1: Initial Attach in satellite network for S&F operation

1-3 Initial Registration Process: Upon entering the satellite's coverage, the UE initiates an Initial Attach Request. The MME-SAT, unable to immediately establish a ground connection, temporarily stores the UE's International Mobile Subscriber Identity (IMSI) and issues an Attach Reject message. The MME-SAT rejects the UE's Initial Attach Request with an Attach Reject message that includes a Cause value indicating that the Attach procedure is suspended, as well as a Timer value(indicating how long the UE should refrain from attempting another Attach).

NOTE: The Cause and the Timer can be protected with a digital signature, which the UE can validate using provisioned root certificates.

Editor’s Note: The impact of using a Certificate is FFS.

4-5 Once MME-SAT establishes contact with MME-GND, it forwards the IMSI to request authentication vectors from the Home Subscriber Server (HSS).

6-10 In subsequent coverage, the UE re-initiates the Attach Request. This time, MME-SAT, equipped with the authentication vectors, proceeds to authenticate the UE, leading to a successful Attach Acceptance. Immediately following successful authentication, MME-SAT sends a provisional Update Location Request to the HSS. This update includes an indicator that the location update is provisional and should not be fully processed until a final confirmation is received, optimizing the handling of location data under intermittent connectivity.

11-12 Location Update Process: MME-SAT updates the UE's location with the HSS upon establishing ground connectivity, ensuring the UE's subscription permits service in the attempted location. Any discrepancies trigger a detach procedure during the next satellite contact.

### 6.9.3 Evaluation

The proposed solution effectively addresses the key security issues identified in Key Issue #1, particularly focusing on the challenges of intermittent connectivity inherent to satellite communications.

The solution introduces a split architecture for the MME, with segments aboard the satellite (MME-SAT) and on the ground (MME-GND). This design accommodates the intermittent connectivity of satellite coverage and facilitates secure communication between the UE and the network. By temporarily storing the UE's IMSI and issuing an Attach Reject message with a Cause value and a Timer, the solution ensures that the UE can only attempt re-attachment after a specified period.

Upon establishing contact with MME-GND, MME-SAT requests authentication vectors from the Home Subscriber Server (HSS), enabling the authentication of the UE in subsequent coverage. This process ensures that the communication between the UE and the network is authenticated and secure, addressing the confidentiality and integrity of the messages. The provisional Update Location Request sent to the HSS immediately after successful authentication includes an indicator that the location update is provisional. This approach optimizes the handling of location data under intermittent connectivity, ensuring that the integrity and confidentiality of control-plane messages are maintained.

Based on the choice of operator(Satellite) implementation, The solution's architecture inherently mitigates potential DoS attacks that could arise from the storage capacity being exhausted by spoofed data. By implementing a digital signature for the Attach Reject message, the network ensures that only UEs with valid credentials can re-attempt attachment, reducing the risk of spoofed data flooding the system. However, it does not address the DoS attack on the storage capacity due to the unprotected message in step 1.

Additionally, the provisional Update Location Request mechanism ensures that the network resources are optimally utilized, preventing unauthorized UEs from exhausting the storage resources on the satellite.

Editor’s Note: Further evaluation is FFS.

## 6.10 Solution #10: UE Attach/Registration method for S&F operation

### 6.10.1 Introduction

This solution addresses Key issue #1: Security protection in Store and Forward Satellite Operation.

The principle of the solution is:

1. UE subscription information is stored in a UE authentication token that is protected by confidentiality and integrity. UEs cannot understand and modify the UE authentication tokens.

2. When the UE connects to a satellite, it provides the UE authentication token to the satellite.

3. The satellite decrypts and verifies the UE authentication token, generates UE subscription data based on the content contained in the UE authentication token, and then authenticates the UE.

There is a valid time in the UE authentication token. Tokens should not be used after their expiration time. Token provision and re provision are implemented at the application layer.

### 6.10.2 Solution details

UE Attach/Registration method for S&F operation is shown in the following figure.



Figure 6.10.2-1: UE context management procedure for S&F operation

0. The LTE/5G system provisions security materials for decrypting and verifying UE authentication tokens to satellites that support S&F operation.

The LTE/5G system generates UE authentication token for a UE. The UE authentication token contains UE subscription information and UE authentication key, which can be used to generate UE subscription data. UE authentication tokens need to be protected by confidentiality and integrity.

The LTE/5G system provisions the UE authentication token to the UE. How to provision UE authentication token is out of the scope of the 3GPP system.

NOTE: What subscription information should be included in the UE authentication token and how to protect it will be specified in the normative phase.

1. When the UE connects to a satellite, it sends an attach/registration request to the satellite, which includes the UE authentication token.

If privacy protection is required, a security mechanism similar to SUCI can be used to protect UE authentication tokens.

2. The satellite decrypts and verifies the UE authentication token using the security materials received in step 0.

3. The satellite generates UE subscription data using the content contained in the UE authentication token.

NOTE: How to handle SQN will be specified in the normative phase.

4. The satellite and the UE continue to perform other attach/registration procedure.

5. The satellite and UE exchange downlink/uplink data through established security connection. After disconnecting, the satellite does not need to save UE context.

### 6.10.3 Evaluation

This solution uses the existing solutions specified in TS 23.401 [9] to achieve authentication and communication security, thus meeting the requirements of Key Issue #1.

The advantages of this method are:

- No changes to the existing authentication and NAS/AS security procedures.

The drawbacks of this method are:

- Token protection keys need to be pre-configured in the satellites.

- Protocol needs to be changed in order to transmit tokens.

## 6.11 Solution #11: UE context management for S&F operation

### 6.11.1 Introduction

This solution addresses Key issue #1: Security protection in Store and Forward Satellite Operation.

The principle of the solution is:

1. After an UE attaches a satellite, the satellite saves the MME UE context in the UE authentication token that is protected by confidentiality and integrity. UEs cannot understand and modify the UE authentication tokens.

2. The satellite sends the UE authentication token to the UE. The satellite does not store the UE context after disconnecting from the UE.

3. When the UE connects to another satellite, it provisions the UE authentication token to the satellite.

4. The satellite verifies the UE authentication token, reconstructs the MME UE context using the content of the UE authentication token, and then performs a NAS SMC for the new connection.

The solution requires a first satellite to store the MME UE context (including security context and GUTI) in a token, and then provide the GUTI and token to a UE.

When a UE is handed over to a second satellite, its MME UE context will also need to be relocated to a second satellite. The UE provides GUTI and token to the second satellite.

The second satellite needs to perform MME relocation using the information carried in the token, and then create a new UE security context in the second satellite. Security information used for MME relocation is provided to the second satellite through the token.

### 6.11.2 Solution details

UE context management procedure for S&F operation is shown in the following figure.



Figure 6.11.2-1: UE context management procedure for S&F operation

0. The 4G system provisions security materials for encrypting and verifying UE authentication tokens to satellites that support S&F operation. The UE authentication token contains MME UE context information for S&F operation and security materials for key handling in S-MME (on board MME) handover in S&F operation. UE authentication tokens need to be protected by confidentiality and integrity.

NOTE: What UE context information should be included in the UE authentication token and how to protect it will be specified in the normative phase.

1. When the feeder link is available, the HSS provisions UE authentication vectors to the satellite that supports S&F operation and is expected to pass the target UEs.

2. When the service link is available, the UE and satellite perform attach procedure.

3. The satellite and UE exchange downlink/uplink data through NAS messages.

4. The satellite generates GUTI and an UE authentication tokens protected by confidentiality and integrity using the security materials received in step 0, and then sends them to the UE. After disconnecting from the UE, the satellite can delete the MME UE context stored in the S-MME.

5. When the UE connects to another satellite, it sends an attach request to the satellite, which includes GUTI and UE authentication token.

6. The satellite decrypts and verifies the UE authentication token using the security materials received in step 0, performs MME handover procedure and NAS SMC procedure with the UE as specified in TS 23.401 [9], and then reconstructs the MME UE context using the information contained in the UE authentication token.

7. The satellite and UE exchange downlink/uplink data through NAS messages

8. The satellite performs the same operations as step 4.

### 6.11.3 Evaluation

This solution uses the existing solutions specified in TS 23.401 [9] to achieve authentication and communication security, thus meeting the requirements of Key Issue #1.

The advantages of this method are:

- After UE successfully accesses the satellite for the first time, it can perform authentication and data transmission processes in any subsequent connection.

- No changes to the existing authentication and NAS/AS security procedures.

The drawbacks of this method are:

- Token protection keys need to be pre-configured in the satellites.

- Protocol needs to be changed in order to transmit tokens.

## 6.12 Solution #12: Authentication for store and forward satellite operation

### 6.12.1 Introduction

This solution addresses Key Issue#1 on Security protection in Store and Forward Satellite Operation.

The solution is based on the EPS architecture. Considering the feeder link’s intermittent unavailability in the S&F Satellite operation, legacy EPS AKA as described in 3GPP TS 33.401 [3] may not be directly applied to such use case. To provide authentication capabilities when feeder link is not available, one possible approach is to have security credentials on the satellite, which enables the AKA procedure between the UE and the satellite. However, there is a security risk that the user security credentials (e.g. root keys) are stored on multiple satellites, for instance, if a satellite is hijacked, the user security credentials on other satellites can also be compromised. To mitigate this risk, the proposed solution takes into account the idea of subscriber key separation mechanism in Annex F “Isolated E-UTRAN Operation for Public Safety” in TS 33.401[3], where different satellites store different user security credentials.

In addition, due to the limited storage on satellites, storing all user subscription credentials in the onboard HSS is challenging and also difficult to manage. Therefore, it is possible that only a subset of UEs have their security credentials in the onboard HSS. If the UE accesses a satellite which has its security credential, the UE can proceed to run the AKA procedure, otherwise the authentication request is rejected due to the lack of UE security credential. Meanchile, the satellite can record the rejected UE and retrieve its security credentials from the ground HSS when feeder link is available. Then, the UE can access the satellite and continue to perform AKA procedure when the service link is available.

The proposed solution follows the assumptions and principles as below:

- The eNB, MME-NT and HSS-NT are placed on board the same satellite.

- The HSS-NTs for multiple satellites use subscriber key separation mechanism in Annex F in TS 33.401[3].

- The HSS-NT may only have security credentials for a subset of users.

- The HSS-NT retrieve the unstored user security credentials from the ground HSS when feeder link is available.

### 6.12.2 Solution details



Figure 6.12.2-1: Authentication for Store and Forward Satellite Operation

The authentication solution for Store and Forward Satellite Operation has the following steps:

1. The UE and the HSS-NTs for multiple satellites use subscriber key separation mechanism descriped in Annex F “Isolated E-UTRAN Operation for Public Safety” in TS 33.401 [3]. For each UE, there is a master key MK for S&F Satellite operation. The master key MK is stored in the UICC, but not in any HSS-NTs. Each HSS-NT is only provisioned with the subscriber keys (i.e., long-term key) derived from the master keys MKs for a subset of users. The HSS-T is provisioned with the the subscriber keys (i.e., long-term key) derived from the master key MK for all users.

NOTE 1: The master key MK can be a root key or a dedicated key exclusively for S&F Satellite operation.

NOTE 2: Assume that there are N satellites with different HSS-NTs, HSS-NT\_1, ..., HSS-NT\_N. As part of the provisioning process for HSS-NT\_n (1<=n<=N), a subscriber key K\_n is derived from MK using the key derivation process specified in Annex F of TS 33.401 [3], and all K\_n are different and the knowledge of K\_n does neither allow inferring knowledge about MK nor about any K\_m with m different from n.

NOTE 3: Due to the limited storage capability, the HSS-NT may only have the subscriber keys for a subset of users.

When service link between UE and SAT#1 is available

1. The eNB on the SAT#1 broadcasts that it is in the S&F satellite operation mode.
2. If the UE has the capability to support the S&F satellite operation, it initiates the Attach procedure by transmitting an Attach Request Message to the eNB including the UE ID, e.g., IMSI. Then, the eNB forwards the Attach Request message to MME-NT.
3. The MME-NT on the SAT#1 sends an Authentication Request message to HSS-NT on the SAT#1 including the UE ID.
4. If the subscriber key is not stored in the HSS-NT on the SAT#1, the HSS-NT sends an Authentication Failure Message to the MME-NT on the SAT#1 including a failure indication.
5. The MME-NT on the SAT#1 sends the Attach Reject message to UE.

When the feeder link between SAT#1 and the ground network is available

1. The HSS-NT on the SAT#1 sends the Security Key Request Message to the HSS-T including the rejected UE’s IMSI and current TAI, and retrieves the subscriber key from the HSS-T.
2. The HSS-T sends Security Key Reponse Message to HSS-NT on the SAT#1 with the subscriber key.

When service link between UE and SAT#2 is available

8~10. Step 8~10 are the same as step 1~3.

11~16. The run of an EPS AKA procedure in step 11~16 in the presence of the subscriber key separation mechanism is identical to that without the presence of the mechanism in clause 6.1 in 3GPP TS 33.401 [3], except for the operation of the step 11 and step 14. The modified operation is described as follows:

1. In step 11, If the HSS-NT on the SAT#2 has the the subscriber key, EPS AKA proceeds as described in clause 6.1 in 3GPP TS 33.401 [3], with the subscriber key replacing the permanent subscriber key in all computations;
2. In step 14, when the UE receives an Authentication Request Message from the MME-NT on the SAT#2, the USIM first derive the subscriber key from the master key using the key derivation process specified in Annex F in TS 33.401 [3], which can be locally stored for future use to improve efficiency. Then, EPS AKA proceeds as described in clause 6.1 in 3GPP TS 33.401 [3], with the subscriber key replacing the permanent subscriber key in all computations.
3. MME-NT on the SAT#2 sends an Attach Accept Message to the eNB. Then, the eNB forwards the Attach Accept message to the UE.

Editor’s note: It is FFS whether the solution can support roaming scenarios.

### 6.12.3 Evaluation

This solution fulfils all the potential requirements in key issue #1 for security protection in S&F Satellite operation.

This solution, by deploying the HSS onboard the satellite, solves the problem of the incomplete AKA procedure due to the feeder link’s intermittent unavailability and enables the regular AKA process between the UE and satellite networks.

This solution proposes to reuse the subscriber key separation mechanism defined in Annex F.4 of TS 33.401[3] for provisioning the different subscriber keys in different satellites for the same UE.

Editor's Note: Further evaluation is FFS.

## 6.13 Solution #13: Security protection based on onboard HSS

### 6.13.1 Introduction

This solution address the key issue#1:Security protection in Store and Forward Satellite Operation.

### 6.13.2 Solution details

This solution based on the solution#18 in the TR 23700-29 [2] with following assumptions and principles:

*- The eNB, MME and HSS are placed on board the same satellite.*

*- The UE has a subscription and credentials in the onboard HSS, the onboard HSS is synchronized with the HSS on the ground when feeder link is available.*

*- Single satellite deployment use case, the UE accesses one satellite only which maintains a NAS and AS state of the UE.*

*- No roaming support.*

Given the above assumption, The authentication and NAS security can be accomplished when service link is available.

The onboard HSS is synchronized with the HSS on the ground when feeder link is available. It is assumed that a subset of UEs have their subscriptions and credentials in the onboard HSS. Different satellite stores distinct subscriptions and credentials for different subsets of UEs. If the UE accesses a satellite which has its subscription and credential, the UE can proceed to attach, otherwise the attach request is rejected due to the lack of UE subscription and credential.

### 6.13.3 Evaluation

TBD

## 6.14 Solution #14: Authorization mechanism for uplink NAS message in S&F satellite operation

### 6.14.1 Introduction

This solution addresses KI#1: Security protection in Store and Forward Satellite Operation.

For delay-tolerant/non-real-time satellite services (i.e. CIoT with Control Plane optimisation, SMS over NAS), only NAS security is activated to perform integrity protection and ciphering for the small user data or SMS. During the feeder link’s intermittent unavailability, the S&F service function on the satellite cannot obtain the UE’s NAS context to verify the uplink NAS data. Thus, a malicious terminal can send a large number of uplink NAS messages to occupy the satellite storage space.

This solution addresses an authorization mechanism to prevent the S&F service function from being flooded with excessive uplink NAS message.

### 6.14.2 Solution details

The Figure 6.14.2-1 describes the detailed authorization mechanism for the uplink data in Store and Forward Satellite Operation.

Editor’s Note: The S&F operation function is a logic module. The architecture will be aligned with SA2’s study.

The ground network will generate one or more one-time password(s) once it received a S&F service indicator from a registered UE. Then, the ground network sends the one-time password(s) to UE and corresponding satellites. The corresponding satellites are determined based on ephemeris. The transmission between AMF\MME and satellite is left to implementation. The ground network can send a timestamp to the satellite optionally which indicate deleting the one-time password after timeout.

During the feeder link unavailable period, if a UE sends an uplink NAS message with an invalid or used one-time password, the satellite drops the uplink NAS message. If a UE sends an uplink NAS message without a one-time password, the satellite regards the UE as an unregistered UE or a legacy UE. As an example, the satellite only offers registration service or emergency service and drops any other uplink NAS messages for OTP-less UE.



Figure 6.14.2-1: Authorization mechanism for the uplink data in S&F Satellite Operation

1. During the registration procedure, the UE sends a S&F service indicator to the MME\AMF. The indicator indicates the UE subscribe the store and forward service.
2. The MME\AMF generate a one-time password based on the S&F service indicator.
3. The network invokes a downlink NAS message. The message includes the one-time password generated in Step 2. The network forwards the one-time password to the satellite which will provide the S&F service for the UE at the feeder link unavailable period.
4. During the feeder link unavailable period, the UE sends an uplink NAS message including data and the one-time password to the satellite.

Editor’s Note: How does the UE know the feeding link status will be aligned with SA2 and it is ffs.

1. After receiving the uplink NAS message, the satellite checks the satellite checks that the fresh one-time password is same as that stored in the satellite before. If the check is successful, the satellite stores the uplink NAS message
2. When the feeder link is available, the satellite sends the uplink NAS message to MME\AMF in ground network.

### 6.14.3 Evaluation

The solution addresses the requirement of KI#1 related to mitigate the potential denial of uplink NAS message attack in the Store and Forward Satellite Operation. The solution requires the EPS/5GS systems forward the one-time password to the UE and satellite(s) after the UE registrates to the EPS/5GS systems successfully. The procedure proposes to use a one-time password for authorization check when a UE sends an uplink NAS message during the feeder link unavailable period. If an uplink NAS message is sent with an invalid one-time password, the satellite will determine to store or drop the uplink NAS message to avoid storing large amounts of uplink data. Thus, this solution mitigates the potential denial of uplink NAS message attack in the Store and Forward Satellite Operation.

Editor’s Note: whether the solution is applicable for legacy UE is FFS.

Editor’s Note: whether a one-time password may be misused e.g., by blocking the transmission of a trustworthy UE and resending the captured one-time password with the wrong payload is for further evaluation.

## 6.15 Solution #15: Attach procedure with eNB on board the satellite

### 6.15.1 Introduction

This solution is proposed to address Key Issue #1, supporting the mutual authentication between the UE and network when the eNB is on board the satellite.

Unlike the attach procedure under normal/default Satellite operation, if the UE attempts to attach to the network under the S&F satellite operation, the network first needs to check whether the UE is authorized to use S&F satellite operation, because an unauthorized UE may launch DoS attack to deplete the resource of the network entities enforcing storing and forwarding. This solution provides a method for the MME to perform the UE authorization before authentication during S&F satellite operation. To be specific, the MME first checks the UE authorization based on the UE subscription information obtained by the HSS. If the UE is authorized, the MME interacts with the HSS to get the authentication vector and sends the authentication request to the UE. Otherwise, the MME stops the attach procedure by sending the attach reject message to the UE.

The proposed solution saves signalling resources and storage resources, ensuring that the eNB on board the satellite and the MME on the ground network do not waste resources to store the signalling/authentication vector for the unauthorized UE.

### 6.15.2 Solution details

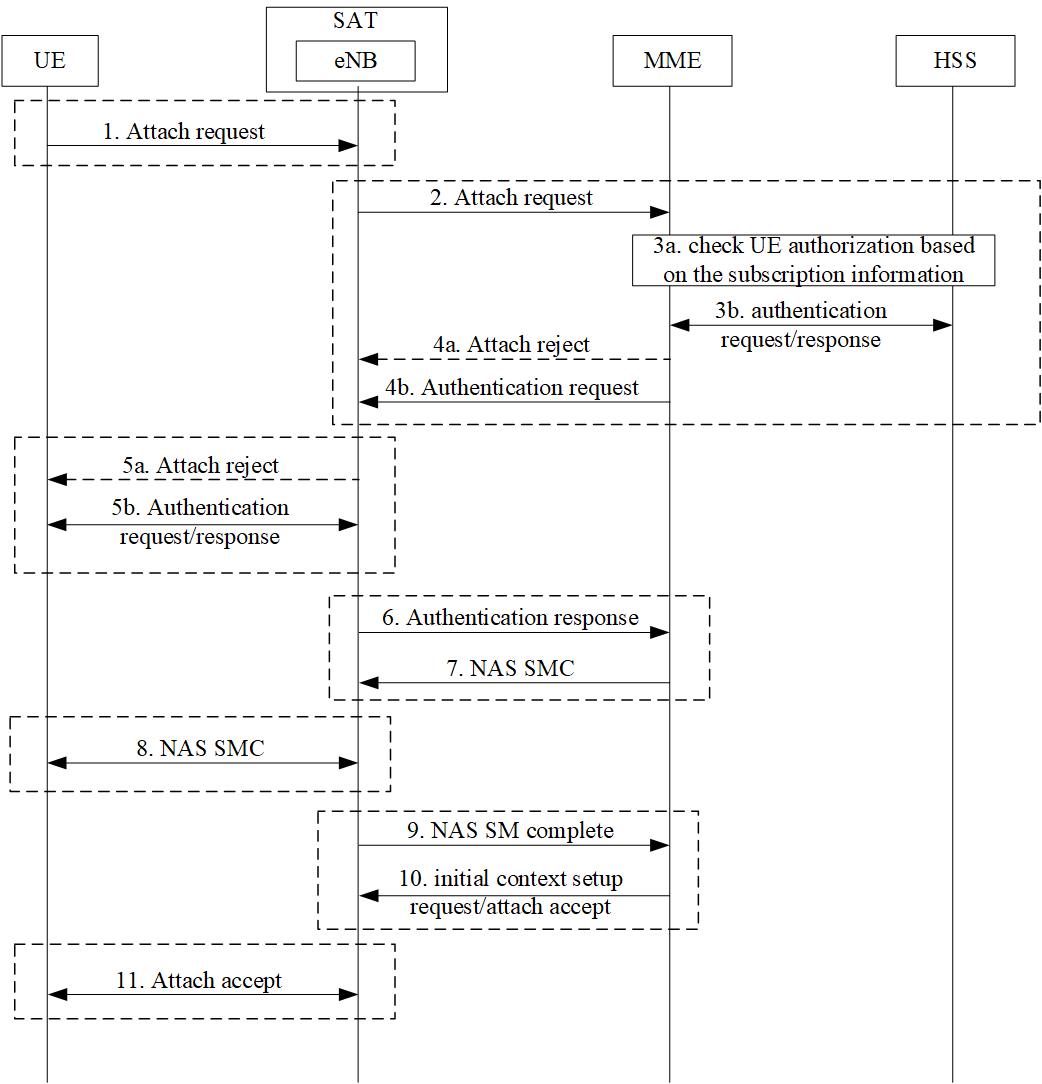


Figure 6.15.2-1: Attach procedure with eNB on board the satellite

1. The UE initiates the attach procedure by sending the Attach request to the eNB which is on board the satellite.
2. If the feeder link is unavailable, the eNB temporary stores NAS signalling from the UE. When the feeder link becomes available, the eNB forwards NAS signalling to the MME, including the S&F indication.
3. The MME interacts with the HSS to obtain the UE subscription information for initiating the authentication procedure.
4. If the UE is authorized to use S&F service operation, the MME returns the authentication request to the eNB. If the UE is not authorized, the MME returns the Attach reject to the eNB.
5. If the service link is unavailable, the eNB temporary stores NAS signalling from the core network. When the service link becomes available, the eNB forwards NAS signalling to the UE, which can be Attach reject message or Authentication request message. If the UE is authorized to use S&F service operation, the step #5b is executed. Otherwise, the step #5a is performed.

If the UE receives Attach reject message, the UE stops the attach procedure and waits to re-initiate the Attach procedure until the satellite can establish the service link and feeder link at same time. Steps 6-11 are skipped.

If the UE receives authentication request message, the UE returns authentication response to the eNB.

1. When the feeder link becomes available, the eNB sends authentication response to the MME.
2. The MME returns NAS Security Mode Command message.
3. When the service link becomes available, the UE performs the NAS SMC procedure.
4. When the feeder link becomes available, the eNB sends NAS SM Complete message to MME.
5. The MME sends the initial context setup request/attach accept.
6. When the service link becomes available, the eNB forwards the Attach accept message to the UE.

NOTE: how to prevent DoS attacks before the security context is established between authorized genuine UE and network is out of scope of this solution.

### 6.15.3 Evaluation

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

## 6.16 Solution #16: Authorization during S&F MO transmission

### 6.16.1 Introduction

This solution is proposed to address Key Issue #1, supporting the authorization during S&F MO data transmission when the eNB is on board the satellite.

This solution provides a method for the eNB to perform UE authorization during S&F MO transmission. Once receiving the MO data request, the eNB on board the satellite determines whether the UE is authorized to use S&F satellite operation based on the UE context. The UE S&F authorization information is included in the UE context, which can be provided by the MME. Only for the authorized UE, the eNB can temporarily store the MO data and forward it when the feeder link becomes available.

The proposed solution ensures the eNB on board the satellite can resist the DoS attack launched by an unauthorized UE. If the unauthorized UE tries to exhaust the storage resource of eNB by sending excessive amounts of MO data, the eNB can detect and reject to accept the storage.

### 6.16.2 Solution details

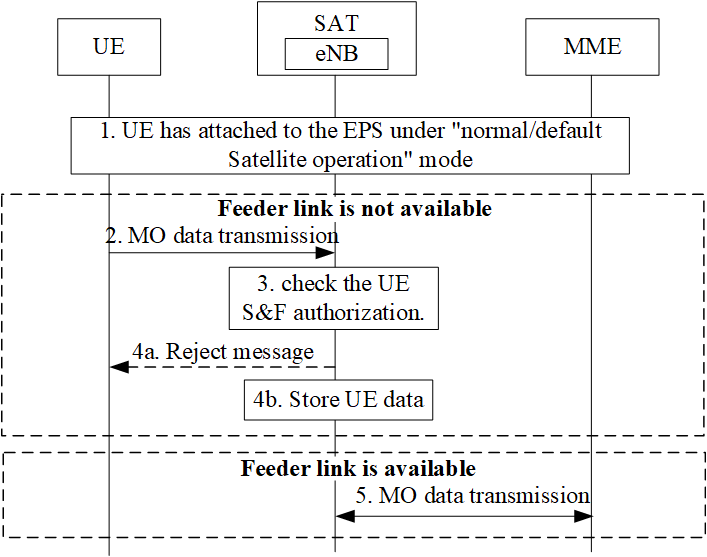


Figure 6.16.2-1: authorization during S&F MO data transmission

1. The UE has attached to the EPS, by performing the attach procedure under "normal/default Satellite operation" mode.

Due to the mobility of satellite after the UE is attached, the feeder link between the eNB on board the satellite and MME on the ground network becomes unavailable and the "S&F Satellite operation" mode is supported by the eNB and MME.

1. The UE sends MO data by using the CP CIoT EPS Optimization or UP CIoT EPS Optimization.
2. Once receiving the MO data, the eNB determines whether the UE is authorized to use S&F satellite operation based on the UE context. The UE context contains the UE S&F authorization information, which is provided by the MME based on the UE subscription information. If the UE S&F allowed geographical area is included in the UE S&F authorization information, the eNB further checks the location of the cell to which the UE is camped to determine whether to accept the MO data. If the UE S&F allowed time period is included in the UE S&F authorization information, the eNB further checks the time of MO data transmission to determine whether to accept the MO data.
3. If the UE is not authorized, the eNB sends reject message, in9dicating the unavailability of feeder link. Once receiving the reject message, the UE stops to send the MO data until both the service link and feeder link become available. If the UE is authorized, the eNB determines to temporarily store the MO data.

NOTE 1: The UE can determine the status of feeder link based on the coverage availability information and/or satellite orbit information.

When the feeder link between the eNB on board the satellite and MME on the ground network becomes available,

1. The eNB forwards the MO data to the MME.

### 6.16.3 Evaluation

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

Editor’s Note: The impact of unprotected Reject message is FFS.

## 6.17 Solution #17: Attach procedure with MME on board the satellite

### 6.17.1 Introduction

This solution is proposed to address Key Issue #1, supporting the mutual authentication between the UE and network when the MME is on board the satellite.

The solution assumes that the AKA procedure is initiated and completed when both the feeder link and service link are available. To ensure this, the MME can leverage the pre-provisioned orbit information. The satellite coverage information or satellite orbit information enables the MME to determine when the both service link and feeder link become available and provide a back-off timer to the UE. Based on the obtained back-off timer, the UE can avoid performing attach in S&F satellite operation by re-initiating and completing the attach procedure after the back-off timer expires.

The proposed solution minimizes the risk of DoS attacks during intermittent AKA procedure and ensures the UE can attach to the network by avoiding performing the procedure in S&F satellite operation.

### 6.17.2 Solution details

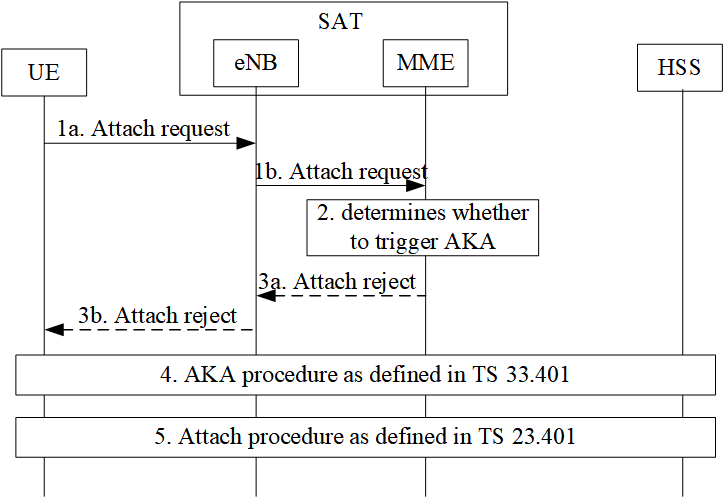


Figure 6.17.2-1: Attach procedure with MME on board the satellite

1. The UE initiates the attach procedure via the eNB on board the satellite.

2. Once receiving the attach request, the MME determines whether to trigger the AKA procedure as defined in TS 23.401 [9]. If the AKA procedure is determined to be initiated and the feeder link is currently not available, the MME calculates the back-off timer and proceeds to step #3. The back-off timer indicates when the feeder link becomes available, which is determined by using the pre-provisioned orbit information of satellite. If the AKA procedure is to be initiated and the feeder link is currently available, step #3 is skipped.

3. The MME sends the Attach reject message including the back-off timer. Based on the received Attach reject message, the UE re-initiates the attach procedure after the back-off timer expires.

4. With both the feeder link and service link available, the MME performs the AKA procedure as defined in TS 33.401 [3].

5. After the AKA procedure is completed, the MME continues the attach procedure as defined in TS 23.401 [9].

NOTE: how to prevent DoS attacks before the security context is established between UE and network is out of scope of this solution.

### 6.17.3 Evaluation

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

## 6.18 Solution #18: Security protection for store and forward satellite operation

### 6.18.1 Introduction

Key issue#1 is addressed by this solution. Currently, integrity protection of the user data between the UE and the on-board RAN node is optional to use. For example, the integrity protection may be not activated by the on-board RAN node based on the security policy or local configuration. Without integrity verification, fake data may be stored in the on-board RAN node.

This solution addresses store and forward Satellite Operation in the delivery of delay-tolerant/non-real-time satellite services (i.e., CIoT UP Optimizations).

### 6.18.2 Solution details

In addition to the UP integrity protection policy, the on-board RAN node also considers whether store and forward Satellite Operation is supported or not when activating UP integrity protection. If supported, the integrity protection is activated as much as possible. For example, if the UP integrity protection policy is “preferred”, the integrity protection will be activated.

If the feeder link is not available, the data after successful integrity verification will be stored with priority in the on-board RAN node. For the priority and process of the data storage, it is left to RAN’s implementation. For example, if the storage of the on-board RAN node doesn’t reach the warning threshold, the data is treated equally. If the storage of the on-board RAN node reaches the warning threshold, only data after successful integrity verification will be stored. RAN can decide to release the PDU session without integrity protection or activate the UP integrity protection based on implementation. In addition, the stored data will still be maintained without impact.

NOTE: how to prevent DoS attacks before the security context is established between UE and network is out of scope of this solution.

Editor’s Note: Whether a UE needs to be made aware of changes in the on-board RAN’s storage behaviour is FFS.

### 6.18.3 Evaluation

This solution addresses store and forward Satellite Operation in the delivery of delay-tolerant/non-real-time satellite services. If only data after integrity verification is stored, the fake data from attacker will be discarded. Based on this, the potential DoS attack is mitigated.

Editor’s Note: additional evaluation is FFS.

## 6.19 Solution #19: Mitigating UE privacy risks using temporary UE ID

### 6.19.1 Introduction

This solution addresses the KI#2.

In TR 23.700-29 [2], some solutions need to assign an interim GUTI to a UE before NAS security is established. However, the interim GUTI is sent in clear text and reused multiple times. Thus, it is possible that the UE can be tracked based on the interim GUTI.

In this solution, it is proposed to use one interim GUTI only once. Besides, the interim GUTI is generated based on the UE’s input in the uplink. The rationale of the solution is as follows.

In a satellite scenario, the downlink traffic is transmitted from the satellite to the UE on the ground whereas the uplink traffic is directed to the satellite. Therefore, it is easier to eavesdrop the downlink messages instead of uplink messages for a passive attacker on the ground.

### 6.19.2 Solution details

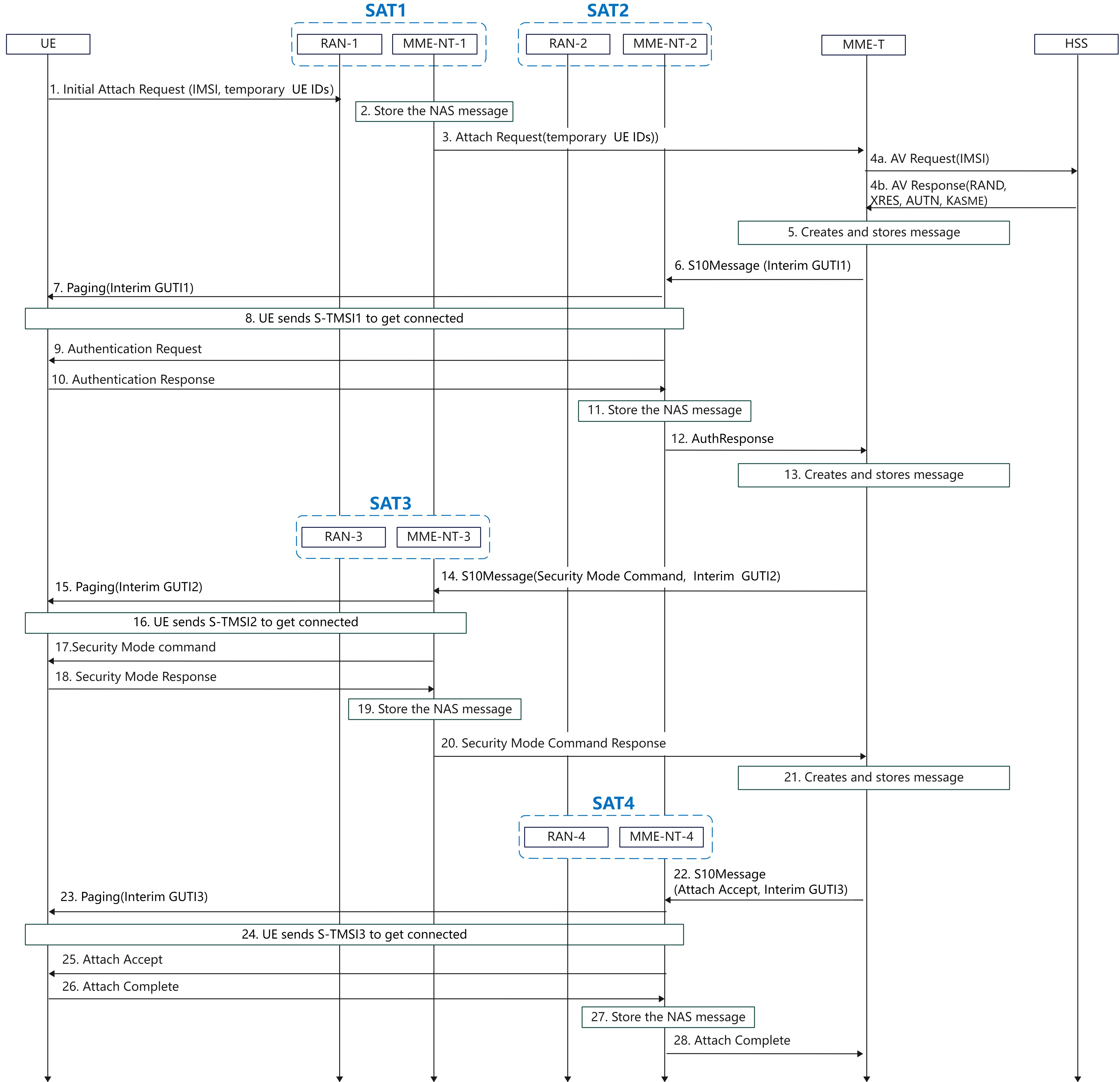


Figure 6.19.2-1 interim GUTI assignment procedure in S&F, 4G

The attach procedure is based on the Solution #11 in TR 23.700-29[2]. The main difference is that in this solution UE provides temporary UE IDs in the initial attach request for the network to generate interim GUTIs.

Step1: The UE randomly generates one or multiple temporary UE IDs. The UE sends the initial Attach Request (IMSI, temporary UE IDs) to the SAT1. If the interim UE IDs are duplicated, the satellite shall require the UE to send new interim UE IDs. So the interim UE ID for the same MME-NT is unique.

Editor’s Note: The impact and potential abuse of UE ID duplication checks is FFS.

Step2-5: These steps are the same as corresponding steps in the Solution#11 of TR 23.700-29[2]. In addtion, the GUTIs are formed based on the temporary UE IDs.

Step6: When the next satellite available, the MME-T creates the Authentication NAS payload and forwards it to the SAT2 with the interim GUTI1.

Step7: The SAT2 pages the UE using the interim GUTI1.

Step8: The UE extracts the temporary UE ID from the received interim GUTI1 and compares it with the stored temporary UE IDs. If success, the UE generates and sends S-TMSI1 to get connected.

Step9-13: These steps are the same as the corresponding steps in the Solution#11 of TR 23.700-29[2].

Step14: When the next satellite available, the MME-T shall relay the Security mode command with the interim GUTI2 to the SAT3.

Step15-16: These steps are similar to the steps 10-11, with the SAT2 replaced with the SAT3.

Step17-21: These steps are the same as the corresponding steps in the the Solution#11 of TR 23.700-29[2].

Step22: When the next satellite available, the MME-T shall send the Attach accept along with the interim GUTI3 to the SAT4.

Step23-24: These steps are similar to step 10-11 with the SAT2 replaced with the SAT4.

Step25-28: These steps are the same as corresponding steps in the Solution#11 of TR 23.700-29[2].

Editor’s Note: how to generate the interim GUTI from the temporary UE ID is FFS.

NOTE: This solution is also applicable to the 5G systems, with the MME replaced with the AMF and the attach procedure with the registration procedure.

### 6.19.3 Evaluation

The solution is addressing the KI#2.

The solution is based on the SA2’s solution #11 with security enhancement. The temporary UE IDs are provided by the UE for the network to generate the interim GUTI so that only the intreim GUTI is not reused to prevent traceability and linkability.

## 6.20 Solution #20: Mitigation of privacy issues of interim GUTI

### 6.20.1 Introduction

The solution addresses the key issue #2 “privacy threats of S&F operation”.

In TR 23.700-29 [2], there are multiple solutions that require SAT to assign an interim GUTI to the UE in an unprotected NAS message, such as solution 11, 12, 13, etc. These solutions propose a similar approach to interim GUTI assignment: after the UE accesses SAT1, an interim GUTI is configured by SAT1 without protection, synchronized to the MME ground, and used for paging the UE by SAT2 when SAT1 is replaced by SAT2. The goal is to ensure the UE is reachable once the stored NAS message is forwarded to the ground MME and sent to SAT2.

However, since the interim GUTI is not ciphered or integrity protected, the following security issues are identified:

1. An attacker can use a FBS to continuously track a UE by assigning an interim GUTI and conducting Paging, allowing them to track the UE's location actively.
2. Intercepting the IMSI and interim GUTI of a UE allows an attacker to determine the UE's approximate location passively.

This solution proposes two alternative solutions to address the issues above.

### 6.20.2 Solution details

For those solutions that assign the interim GUTI without protection, the general procedure is as depicted in figure 6.20.2-1:

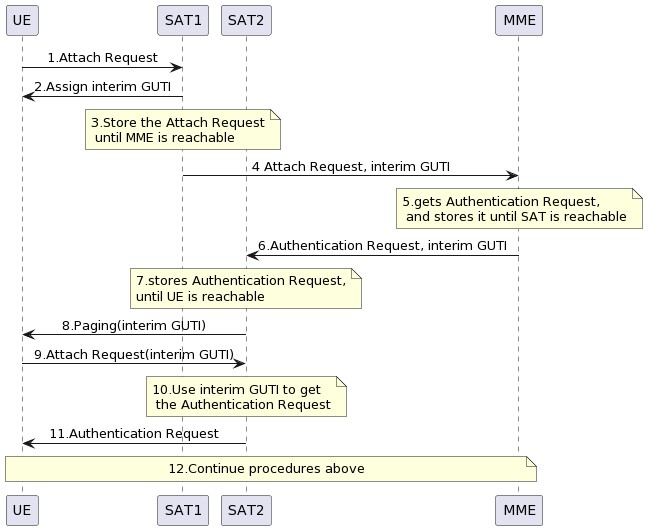


Figure 6.20.2-1 General procedure of interim GUTI assignment solutions

1. The UE sends the Attach Request message to SAT1.
2. The SAT1 assigns an interim GUTI to the UE in case of a connection loss with SAT1. The UE will store the interim GUTI.
3. The SAT1 stores the Attach Request until ground MME is reachable.
4. The SAT1 sends the Attach Request message with the interim GUTI to the ground MME.
5. The ground MME sends the Authentication Data Request message to the HSS, and gets Authentication Data Request, the ground MME constructs Authentication Request message and stores it until SAT is reachable.
6. If a new connection between SAT2 and the ground MME is established, the MME then sends the Authentication Request message with the interim GUTI to SAT2.
7. The SAT2 stores the Authentication Request message until the UE is reachable.
8. The SAT2 uses the interim GUTI to page the UE.
9. The UE who stores the interim GUTI will reply back to the SAT1 by sending the Attach Request with the interim GUTI.
10. The SAT2 uses the interim GUTI to find the stored Authentication Request message.
11. The SAT2 sends back the Authentication Request message to the UE.
12. The UE and the network continue the procedures above to finish the attach procedure.

Two alternative solutions based on the procedure above are introduced to address or mitigate the security issues as described in clause 6.20.2.1 and 6.20.2.2.

#### 6.20.2.1 Alternative 1: restrict the use of interim GUTI

Alternative 1 is to restrict the use of interim GUTI in order to minimize its impact.

The interim GUTI shall have a short validity period and be strictly limited to the S&F scenario.

To achieve a short validity period, the following mechanisms can be implemented:

1. Once a new GUTI is assigned from a protected NAS message, the interim GUTI becomes invalid.
2. Once a timer expires, the interim GUTI shall be invalid.

To enforce scenario limitation, when the UE store the interim GUTI in step 2 or use it in step 8 or 9, the UE shall ensure it is in S&F operation.

Alternative 1 restricts the use of interim GUTI exclusively to S&F operations, thereby confining the identified security issues to a short period of time, such as during the attach procedure.

#### 6.20.2.2 Alternative 2: No use of interim GUTI

Alternative 2 proposes not to use the interim GUTI. The network side just stores the association between IMSI and DL NAS message, and uses the IMSI for paging.

The following steps are impacted:

1. Step 2 is not needed.
2. In step 4 and 6, the interim GUTI is replaced by IMSI.
3. In step 8 and 9, the SAT2 uses IMSI for paging.

Alternative 2 proposes to use IMSI for paging which is feasible in 4G, but it cannot inherit to 5G.

### 6.20.3 Evaluation

The solution has little additional impact based on SA2 solutions that assign an interim GUTI to the UE in an unprotected NAS message.

Alternative 2 reuses LTE solution and has the same security level with LTE.

Editor’s Note: More security analysis of alternative 1 and alternative 2 is ffs.

## 6.21 Solution #21: Remediation of unauthenticated (D)DOS in S&F

### 6.21.1 Introduction

This solution addresses requirement #3

*The 3GPP system shall support means to mitigate the potential denial of service attack in the Store and Forward Satellite Operation.*

in Key Issue #1: Security protection in Store and Forward Satellite Operation, of the present document

This solution assumes that a satellite in S&F a Service Link (SL) is available, and the Feeder Link (FL) is temporarily unavailable.

When SL and FL are not available at the same time, the satellite in S&F mode has to store NAS or AS data on board of satellite. This condition can lead to the exhaustion of storage and processing resources on board the satellite in S&F mode.

When an unauthenticated UE attempts to register, a satellite in S&F mode will need to store the registration request until the FL becomes available. This condition can be exploited by fraudulent UEs mounting a (D)DOS attack. Backoff timer and throttling are effective means to remediate (D)DOS attacks post-authentication.

This contribution proposes a solution for the remediation of unauthenticated (D)DOS in S&F.

Registration Requests can be easily spoofed by attacker(s) generating a massive number of such requests. The proposed solution is based on the idea of slowing down the rate of Registration Requests from unauthenticated UEs and it is somewhat similar to the use of CAPTCHA in WEB access. The entity that is issuing the Registration Request (i.e., a legitimate UE or an attacker) is asked to perform a kind of action that is intended to slow down the rate of the Registration Request issuance.

Such action is more expensive to perform for the entities whose goal is to issue massive amounts of such requests (i.e., an attacker) than for a legitimate UE. As a result, this solution is disproportionally affecting the attacker.

### 6.21.2 Details

The simplified call flow associated with the proposed solution is presented below.



Figure 6.21.2-1: Call flow for Solution #X: Remediation of unauthenticated (D)DOS in S&F

Steps associated with the call flow in Figure 6.21.2-1:

1. UE issues Registration Request as per Registration Procedure as per TS 23.501 Figure 4.2.2.2.2-1: Registration procedure

2. The equipment on board of satellite, (either eNB/MME or gNB/AMF) senses that there is no available Feeder Link (FL) and decides to provide a puzzle-based (D)DOS remediation

3. The equipment on board of satellite, (either eNB/MME or gNB/AMF) composes a puzzle to be solved by the UE before propagating the Registration Request further in the operator’s network

4. The equipment on board of satellite, (either eNB/MME or gNB/AMF) forwards the puzzle to the UE

5. The UE solves the puzzle and produces the evidence

6. The UE re-issues the Registration Request with the evidence of solved puzzle

7. The equipment on board of satellite, (either eNB/MME or gNB/AMF) verifies the evidence and checks for the optional freshness.

Editor’s Note: It is FFS whether the additional workload that this solution (i.e., steps 2 – 4, and 7) proposes for the Network Nodes and NFs on board of satellite can be an acceptable tradeoff for remediation of (D)DOS attack.

Editor’s Note: It is FFS how to reduce latency due to the additional round trip.

8. The satellite detects the FL availability

9. The equipment on board of satellite, (either eNB/MME or gNB/AMF) forwards the Registration Request to the land-based CN authentication functionality (e.g., AUSF/UDM)

10. The S&F Registration Procedure continues with steps (4 or 5) as per TS 23.501 Figure 4.2.2.2.2-1: Registration procedure

#### 6.21.2.1 Puzzles

A puzzle can be any cryptographic primitive (encryption, hash function, etc.) that would require brute brute-force attack to reverse.

#### Solving an Encryption Reversing puzzle example

Solving an encryption reversal puzzle is based on the “brute-force” method and it comprises finding plaintext or partial plaintext with either no encryption key knowledge, partial key knowledge, or reduced key size.

Note that processor productivity has an outsized effect on the time/effort needed to reverse encryption.

The procedure of solving this puzzle type is built around going through all existing permutations of the whole encryption key while knowing the partial encryption key. The process diagram is produced in Figure 3.



Figure 6.21.2.1-1: Solving an Encryption Reversing Puzzle

The steps in Figure 6.21.2.1-1 are reflected below:

1. Start of the procedure

2. The UnEn receives the puzzle and corresponding parameters from the ENN. The puzzle and the parameters correspond to what was generated in the procedure of Figure 2 step 10. This step corresponds to step 4 of Figure 1.

3. UnEn selects the initial (e.g., the starting value of the unknown part of the encryption key and uses it together with the known part of the key

4. UnEn executes the encryption function

5. UnEn checks if the encryption is brute-forced (e.g., if the brute-forced cleartext contains the optional known clear text corresponding to the input in Figure 2, step 3).

6. If No, the UnEn increments the unknown part of the key, uses that part together with the known part, and tries to brute-force the encryption again in step 4. If Yes, the process proceeds to step 7.

7. The evidence is comprised of the solved (i.e., brute-forced) encrypted text. The UnEn sends the evidence to the ENN. Sending the evidence corresponds to step 6 of Figure 1.

8. End of the procedure

#### Solving a one-way cryptographic hash function reversing puzzle example

Solving a one-way cryptographic hash function (e.g., SHA-256) reversing puzzle is based on the “brute-force” method and it comprises finding the complete hash function input text with only partial input hash function argument knowledge.

Increasing/decreasing the proportion between known and unknown portions of the hash function input can modulate the strength of the puzzle and the amount of work/effort that an entity (e.g., a UE) has to spend to solve it

RAM productivity has an outsized effect on the time needed to reverse the hash function.

The partially known argument to the cryptographic hash function will be the input parameter. For example, when using SHA-256 cryptographic hash, the input string to the hash has a total length of N and a known input length of N-m. The hash output is provided as one of the input parameters (stated length of 256 for SHA-256). It is the m-bits of the input to the hash function that are not known and comprise the puzzle. The effort will be needed to use a brute-force attack and discover the unknown m-bits of input, so that output = HASH-256 (known input || unknown input)

Evidence produced in the process of solving the puzzle comprises the full length of hash input.



Figure 6.21.2.1-2: Solving a Hash Function Reversing Puzzle

The steps in Figure 6.21.2.1-2 are reflected below:

1. Start of the procedure

2. The UnEn receives the puzzle and corresponding parameters from the ENN. The puzzle and the parameters correspond to what was generated in the procedure of Figure 2 step 10. This step corresponds to step 4 of Figure 1.

3. UnEn selects the initial (e.g., the starting value of the unknown part of the hash input and uses it together with the known part of the hash input

4. UnEn executes the hash function

5. UnEn checks if the hash is brute-forced (e.g., if the hash output corresponds to the whole hash input)

6. If No, the UnEn increments the unknown part of the hash input, uses that part together with the known part, and tries to brute-force the hash again in step 4. If Yes, the process proceeds to step 7.

7. The evidence is comprised of the solved (i.e., brute-forced) complete hash input text. The UnEn sends the evidence to the ENN. Sending the evidence corresponds to step 6 of Figure 1.

8. End of the procedure

### 6.21.3 Evaluation

This solution proposes a method for remediation of unauthenticated (D)DOS in S&F.

Editor’s Note: Further evaluation is FFS.

## 6.22 Solution #22: AS security context establishment with store-and-forward operations

### 6.22.1 Introduction

This solution proposes the following:

* Establish a (selective) SAT Group/constellation. Every Satellite which is maintaining a Service link to a UE/IoT acts as the primary-SAT and is establishing a communication to other neighbour Satellites. The primary-SAT establishes Satellite Group/constellation which is used to transfer UE/IoT contexts and/or Data. In case the UE/IoT and/or Satellite is moving, then the primary-SAT ‘role’ also moves to the new primary-Satellite. AMF can select other satellites to page the UEs. And other satellites forward the paging request to the right satellite too.

1. Alternatively, or additionally, selective SAT Group information is made aware at the AMF. So that AMF can select single alternative satellite to page the UE.

### 6.22.2 Solution details

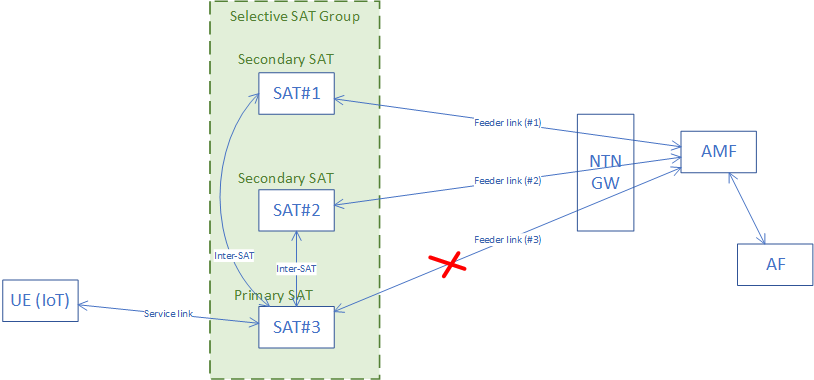


Figure 6.22.2-1: Introduction of selective SAT group

The Application Functions (AF) for some reasons might need to connect to a specific UE (IoT), because the AF wants to share data for instance. For this purpose, the UE (IoT) needs to be paged. The UE (IoT) paging procedure will need to be triggered by the AMF.

The AMF is connected to different satellites (SAT#1, SAT#2, …) and the UE (IoT) is connected to SAT#3 (for instance). Now if we assume the AMF is sending paging information for UE (IoT), BUT the Feeder link to the SAT#3 is not available (=active). In this case the AMF cannot reach out to the UE (IoT) on a direct path.

The UE (IoT) is connected to the SAT#3, but the SAT#3 has no Feeder link active.

The SAT#3 is acting as Primary SAT (pSAT) and is establishing a Selective SAT Group. This selective SAT group (SSG) consists of at least two satellites, i.e., one Primary SAT and another one Secondary SAT. New satellites can be added to the Selective SAT group or existing can be removed. The pSAT is maintaining an inter-SAT communication to every secondary SAT (star-topology). This star-topology is a logic inter-SAT deployment, i.e., every SAT that is maintaining an active Service link to a UE (IoT) is acting as a primary SAT.

This can be seen as a logical meshed deployment.

(1) The UE (IoT) is connected via a service link with SAT#3. The SAT#3 is acting as the primary SAT for this one UE (IoT). The SAT#3 is owning the KgNB and is generating all relevant keys according to the key-hierarchy defined by TS 33.501.

(2) The primary SAT#3 is establishing a Selective SAT Group and is setting up connections to all satellites which are belonging to this Selective SAT Group.

(3) The SAT#3 does not have any longer an active Feeder link.

(3a) The SAT#3 is sending notifications to all SAT Group members and is informing about the missing/inactive (own) Feeder link. The SAT#3 is managing any keys that need to be shared with SAT group members in case of UE handover. This information exchange is via RRC.

(4) The AMF is triggering paging procedure for the UE (IoT) via all the active Feeder link(s). In this deployment scenario the AMF is sending paging messages towards SAT#1 and SAT#2.

(5) The SAT#1 and SAT#2, both Satellites, receive independent the paging request for UE (IoT), both are paging the UE (IoT) within their own ‘tracking area’.

(5a) The SAT#1 and SAT#2, both Satellites send a Paging Request towards the SAT#3. Due to this, the SAT#3 is receiving both paging requests and is triggering paging for that UE (IoT) device in own ‘tracking area’. This paging message is via XnAP.

(6) The UE (IoT) is receiving the paging request and is responding with a Random-Access Procedure.



Figure 6.22.2-2:

(1) The UE (IoT) is connected via a service link with SAT#3. The SAT#3 is acting as the primary SAT for this one UE (IoT). The SAT#3 is owning the KgNB and is generating all relevant keys according to the key-hierarchy defined by TS 33.501.

(2)The primary SAT#3 is establishing a Selective SAT Group and is setting up connections to all satellites which are belonging to this Selective SAT Group. The SAT#3 informs AMF about the Selective SAT Group. i.e., for SAT#3, SAT#1 and SAT#2 are backup. AMF stores this information.

(3) The SAT#3 does not have any longer an active Feeder link.

(3a) The SAT#3 is sending notifications to all SAT Group members and is informing about the missing/inactive (own) Feeder link. The SAT#3 is managing any keys that need to be shared with SAT group members in case of UE handover. This information exchange is via RRC.

(4) When AMF wants to trigger the paging procedure for the UE (IoT) and finds out that SAT#3 is not accessible, then the AMF triggers paging procedure for the UE (IoT) via any one SAT available in the Selective SAT Group with active Feeder link(s). In this deployment scenario the AMF is sending paging messages towards SAT#1 (or SAT#2).

(5) The SAT#1 (or SAT#2) Satellite receive the paging request for UE (IoT), SAT#1 pages the UE (IoT) within their own ‘tracking area’.

(5a) The SAT#1 Satellites sends a Paging Request towards the SAT#3 as well. Due to this, the SAT#3 is receiving a paging request and is triggering paging for that UE (IoT) device in own ‘tracking area’. This paging message is via XnAP.

Editor’s Note: The meaning of own ‘tracking area’ in the selective SAT group/constellation and whether it is related to UE location is FFS.

(6) The UE (IoT) is receiving the paging request and is responding with a Random-Access Procedure.

Editor's Note: This solution relies on communication over ISL.

Editor's Note: How to establish and manage the SAT group is FFS.

Editor’s Note: How the solution aligns with current 3GPP standards, and what are the implications for backward compatibility is FFS.

Editor’s Note: How the solution safeguards against potential security vulnerabilities in the key sharing process over ISL is FFS.

### 6.22.3 Evaluation

Editor’s Note: Whether this solution is aligned with SA2 is FFS.

Editor's Note: Further evaluation is FFS.

## 6.23 Solution #23: Security protection in S&F satellite operation with RAN on board

### 6.23.1 Introduction

This solution addresses KI#1. It applies to an architecture when RAN is deployed in the satellite.

When the Control Plane Optimisation for IoT service procedure is used to exchange delay-tolerant/non-real-time satellite services as payload of a NAS message in both uplink and downlink directions. For the MT control plane data transfer in S&F operation mode, as there is no AS security available in the RAN onboard, and the feeder link’s intermittent is unavailability, the RAN may send the DL NAS message to a malicious terminal.

This solution proposes to protect the RRC connection procedure via using NAS parameters from core network, then the RAN is able to know whether it is talking to a genuine UE.

### 6.23.2 Solution details

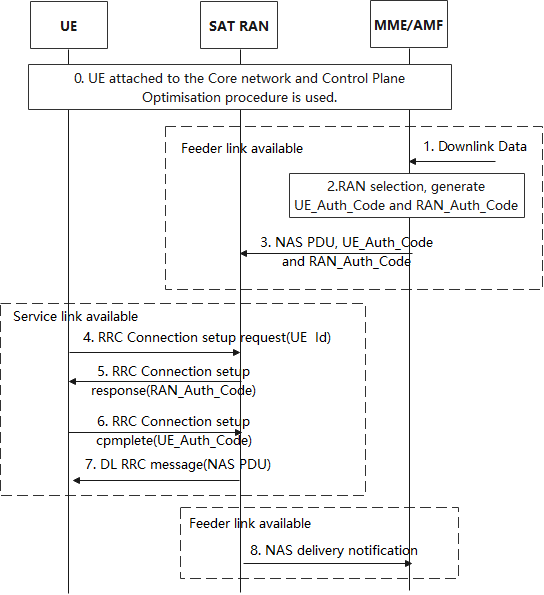


Figure 6.23.2-1:Security procedure for the DL NAS message in S&F Satellite Operation

To protect the RRC connection procedure for DL NAS message delivery, the following procedure is preceded:

0. UE attached to the core network and control plane optimisation procedure is used.

1. The AMF/MME receives downlink data.

2. The MME/AMF determines that the UE is working in S&F mode, the MME selects suitable RAN node, and generates UE Auth\_code and RAN\_Auth\_code by using the currently used NAS integrity algorithm with the following inputs, KNASint as the key, the downlink NAS COUNT that would be used for the next uplink NAS message and the RAN node Id as the message to be protected to calculate NAS-MAC. The first 16 bits of NAS-MAC form UE Auth\_code and the last 16 bits form RAN\_Auth\_code.

The MME also prepares the downlink NAS PDU to send to the UE

3. When the feeder link is available, the MME/AMF sends the NAS PDU with UE Auth\_code and RAN\_Auth\_code to the selected RAN node.

4. When the service link between the selected RAN and the UE becomes available, the UE send RRC connection setup request with UE id.

5. The RAN gets the RAN\_Auth\_code based on the received UE Id, and responses to UE with RRC connection setup that including the RAN\_Auth\_code.

6.The UE uses the same mechanism to generate the UE Auth\_code and RAN\_Auth\_code, and verify the received RAN\_Auth\_code. If the verification is successful, the UE sends the RRC connection setup complete to the RAN node with UE\_Auth\_code.

7. The RAN node checks that the received UE\_Auth\_code equal to the stored UE\_Auth\_code, if so, the RAN shall send the DL RRC message with NAS PDU.

8. When the feedlink is available, the RAN node sends NAS delivery notification to the MME/AMF.

Editor’s Note: The potential misuse of RAN\_Auth\_code and UE\_Auth\_code by an attacker is FFS.

### 6.23.3 Evaluation

This solution addresses the Key Issue #1, and it applies for S&F operations in EPS and 5G.

This solution fulfils the security requirement about the mutual authentication between the UE and RAN before transfer the NAS message.

In this solution, the AMF/MME needs to derive UE Auth\_code and RAN\_Auth\_code when determines to send NAS message to UE, and it sends the NAS message to RAN with UE Auth\_code and RAN\_Auth\_code when the feeder link is available. When the service link is available, the UE generates UE Auth\_code and RAN\_Auth\_code using the same method with the AMF/MME.

With this approach, the NAS PDU will not be sent to a malicious terminal.

## 6.24 Solution #24: Expedited Authentication in 5GS in S&F Mode

### 6.24.1 Introduction

This solution addresses “Key issue #1: Security protection in Store and Forward Satellite Operation”.

The solution proposes to address & optimize security aspects of solution #12 and #15 in 3GPP TR 23.700-29 (albeit for 5GS). The solutions assumes that AMF functionality is broken down into an AMF on-board (called AMF') and an AMF on-ground (called AMF). AMF on-ground maintains UE/Security context, assigns GUTI and uploads UE information in AMF' of next satellite that will fly over the UE's location. AMF' on-board acts as a proxy and provides local termination of NAS on the satellite. It downloads UE context into AMF on-ground when feeder-link is available.

The solutions proposes to pre-fetch authentication information into next satellite that will fly over UE's location.

Authenticaiton and establishment of security context during initial registration suffer from following issues in case of S&F Mode:

* 5GS introduces home control of UE's authentication, whereby the result of authentication is verified by home-network before SUPI and KSEAF are provided to serving-network. In case of S&F mode this would mean following: After Authentication Req/Rsp, AMF' of the current serving satellite needs to store Authentication result (RES\*) and send it to AUSF when it gains feeder-link connectivity. This means two issues:
  + Another satellite pass is required before UE can be successfully authenticated.
  + UE loses radio connectivity while waiting for completion of authentication procedure. In the current scheme of things, the UE may consider that registration procedure has failed and may restart registration procedure during next pass of satellite.
* After successful authentication, the AMF on-ground will then need to upload the authentication response into AMF' of next satellite that flies over the UE, so that it can proceed with Security Mode procedure. After successful establishment of security context, AMF' needs to perofrm Nudm\_UECM / Nudm\_SDM procedures before sending Registration Accept to the UE. This means two issues:
  + These procedures further require connectivity to ground station, and hence another pass of satellite.
  + Waiting for next satellite above means UE loses radio connectivity. In the current scheme of things, the UE may consider that registration procedure has failed and discard the security context if it doesn't receive Registration Accept with a GUTI. In the next pass of satellite, it may restart the registration procedure.

Accordingly, the solution proposes following optimizations to authentication proceure when UEs try to connect to 5G network in S&F Mode:

* Expedited Authentication (Similar to 4GS): XRES\* and KSEAF are provided to AMF/AMF' during Nausf\_UEAU\_Auth Request/Response so that AMF' can validate the result locally and proceed with security mode procedure immediately.
* AMF' sends a (partial) registration accept to the UE containing 5G-GUTI before it performs Nudm\_UECM procedure.

### 6.24.2 Solution details

Consider Figure 6.X.2.1 which details of how the above enhancements help expedite registration/ authentication/ security-mode procedures, while reusing most of existing procedures.

**At time T1,** Sat#1 has Service-Link to the UE, but does not have simultaneous Feeder-Link to the 5GC.

Step #1: The UE initiates a registration request towards the gNB on-board the satellite. The request contains UE Identity set to Subscriber Concealed Identifier (SUCI). The gNB on-board forwards the request to the AMF' on-board.

Step #2: Since the AMF' on-board does not have authentication data to authenticate the UE, as it cannot contact the AUSF/UDM which are on-ground (due to absence of Feeder-link at this point of time), it rejects the registration request and sends the rejection message to UE via gNB (SA2 may decide to use another message, but that should not impact this solution).

The Registration Reject message contains a UE Temporary Identity (e.g. T-GUTI) generated by the AMF'. This identity would be included by the UE in future registration requests, and would be used by AMF' to correlate the UE to the one for whom it would have pre-fetched authentication information using the older SUCI.

Editor's Note: Since the temporary-identity is provided unprotected, it is FFS if such an identity may be used to launch DoS attacks.

Step #3: The AMF' stores the registration request it had received, so that it can intimate to the ground station later, that a UE identified by SUCI is trying to register and its authentication information needs to be made available to next satellite which will fly over UE's location. It also stores the information received over NgAP interface, e.g. the UE's location.

**At time T2,** Sat#1 has moved away and now has Feeder-link connectivity to the ground. At the same time, Sat #2 now has moved to provide Service-link connectivity to the UE.

Step #4: At this point of time, Sat#2 may not have pre-fetched authentication information for the UE. If the UE sends registration request to the gNB on-board Sat#2, it will be rejected similar to Step #3. If the UE had included T-GUTI assigned by Sat#1, Sat#2 should avoid assigning a new temporary identity to the UE.

Step #5: AMF' on-board the Sat#1 sends the Registration Request to the AMF on-ground. The request includes the SUCI as (was) received, T-GUTI assigned by AMF' and the location (e.g. tracking area) where UE was located when registration request was received. If the AMF' determines that UE is operating in S&F Mode, the same may be included in the request to AMF.

Step #6: AMF sends Nausf\_UEAuthentication\_Authenticate Request message to the AUSF to retrieve authentication information for authenticating the UE. The request includes an S&F Indication to signal to the AUSF that the UE is working in S&F mode and is connected via Satellite RAN, and hence an expedited/specialized authentication procedure needs to be initiated which requires lesser back-and-forth exchange of messages with the UE. AUSF may work with UDM to fetch the required information.

Step #7: The AUSF responds back with authentication information to AMF, which includes authentication vectors and the keys (e.g. KSEAF) to be used for driving further keys for protection of messages with UE.

Additionally, AUSF may include XRES\* in the response so that AMF itself can perform authentication validation.

Step #8: The AMF determines the next satellite which will fly over the UE's last known location as provided by AMF' and uploads the authentication information into the AMF' of that satellite (e.g. Sat#3). Thus, the authentication information is pre-fetched into the satellite, ready to handle the future registration request. The information includes the T-GUTI as received in Step #5. The message may also include a 5G-GUTI assigned by the AMF, to be assigned to UE if authentication is successful.



Figure 6.24.2-1: Expedited Registration Procedure

**At time T3**, Sat#2 has moved away and Sat#3 now has Service-link connectivity to the UE.

Step #9: The UE sends Registration request to the gNB on-board Sat #3, including the T-GUTI assigned earlier. gNB forwards it to AMF' on-board.

Step# 10: The AMF' determines it has pre-fetched authentication information (e.g. authentication vectors) of the UE and initiates authentication procedure. AMF' can validate the RES\* if the same was provided by AMF. Else, the AMF' may store the RES\* provided and send to AUSF later when it regains Feeder-link connectivity.

Step #11: This is followed by Security Mode Command/Complete.

Step #12: At this point of time, the AMF' cannot proceed with location update procedure with the UDM on-ground, as Feeder-link is not available. It instead sends a Downlink NAS to the UE, containing a 5G-GUTI received from the AMF on-ground in Step #8. The assignment of the 5G-GUTI at this stage is an indication to the UE that it should save the security context for future use.

The message could be a Partial Registration Accept, whereby the Registration Accept message is enhanced to indicate that it is a partial accept for successful establishment of security context, but the subscription validations are pending.

The UE acknowledges the Downlink NAS message.

**At time T4**, Sat#3 has moved away and regains Feeder-link connectivity to the ground station.

Step #13: The AMF' on-board Sat#3 downloads UE-context into the AMF on-ground. The request includes the 5G-GUTI, and may include the RES\* received from the UE. The request also includes the security context of the UE, generated as a result of security mode procedure executed earlier.

Editor’s Note: Alignment with existing 5G-AKA is FFS.

Step #14: The AMF sends Nausf\_UEAuthentication\_Authenticate Request message to the AUSF.

Step #15: AUSF may validate the authentication result and sends Nausf\_UEAuthentication\_Authenticate Response message to the AMF. If the authentication is successful, the response includes SUPI of the UE.

Step #16: The AMF performs Location Update procedure towards UDM, which may include Nudm\_UECM and Nudm\_SDM procedures as defined in 3GPP TS 23.502 Clause 4.2.2.2. This is followed by subscription validation etc.

Step #17: The AMF determines the next satellite which will fly over the UE's location (e.g. Sat #4) and uploads Registration Accept message into the AMF' of that satellite. The message may include a new 5G-GUTI, or AMF may continue to use the 5G-GUTI already assigned. The message also includes the security context of the UE as received in Step #12.

**At time T5**, Sat #4 has moved over the UE and gains Service-link connectivity to the UE.

Step #18: If UE received a Partial Registration Accept in Step #11, the AMF' inform the UE of Registration procedure completion so that UE can proceed with next steps (e.g. data transfer). This step is optional,

Thus, the UE is able to perform Registration to the network in a two passes of satellite, with minimal changes to existing procedure.

### 6.24.3 Evaluation

Editor’s Note: Impact to the AKA procedure is FFS.

TBD

## 6.25 Solution #25: Solution on preventing DoS attacks before security context is established

### 6.25.1 Introduction

This solution addresses key issue #1: Security protection in Store and Forward Satellite Operation.

In store and forward operation, a satellite receives and stores the uplink data from UEs when only service link is available, and then the satellite forwards the data to the ground network when the feeder link becomes available. For example, the satellite may receive a number of registration request messages from malicious UEs, due to this store and forward property. The storage capacity of the satellite can be easily exhausted, which leads to DoS attack on the satellite. In S&F operation, moreover, UE is vulnerable to a fake satellite attack on the Attach Reject message as captured in some solutions in TR 23.700-29 [2].

In this solution, before the NAS/AS security context is established between the UE and network, key (KSAT.UE) derived from the permanent key is used for the authentication between UE and satellite, in order to prevent the DoS attack and false satellite attack. In this solution, it is assumed that a satellite includes eNB and the functionality of MME related to the authentication called MME (NT).

### 6.25.2 Solution details



Figure 6.25.2-1: Protected attach procedure with MME onboard the satellite in S&F operation

To prevent DoS attacks, the following procedure is preceded:

0. The satellite generates SAT.Nonce and provides it to HSS in GND. The HSS in GND derives KSAT.UE using the permanent key of the UE, ID of the eNB, and SAT.Nonce. The HSS provides KSAT.UE and IMSI to the satellite, and the satellite stores them with SAT.Nonce.

NOTE: The permanent key may be uniquely assigned for S&F operation.

Editor’s Note: How to determine the scope of UEs that need KSAT.UE is FFS.

Editor’s Note: Whether the permanent key should be stored in ME or USIM is FFS.

After that, the authentication process of S&F mode is as follows.

PHASE 1. (Service link is available, Feeder link is unavailable)

1. The satellite provides a random number generated by the satellite (SAT.RN), S&F indicator indicating that the satellite is operating in S&F mode, and SAT.Nonce. These may be included in the SIB (System Information Broadcast) message.

Editor’s Note: Whether SIB messages are only the source of freshness are FFS.

2. The UE derives KSAT.UE using the permanent key of the UE, ID of the satellite, and SAT.Nonce. The UE initiates the attach procedure by transmitting protected Attach Request message. This message consists of the Attach Request message (UE.RN, SAT.RN, and S&F indicator in addition to existing parameters) and MAC of the message, generated by the UE using KSAT.UE. S&F indicator indicates that the UE will operate in S&F mode.

The satellite checks the validity of the UE by verifying the MAC.

3. If the verification is successful, the satellite stores the received attach request message and transmits the protected Attach Reject message. This message consists of the Attach Reject message (Re-attach Info in addition to exsting parameters) and MAC of the message generated by the satellite using KSAT.UE. The Re-attach Info is information necessary for the UE to attempt the reconnection in step 7 (e.g., information about when the UE should retry to reconnect or list of satellite(s) that the UE should retry to reconnect).

The UE checks the validity of the satellite by verifying the MAC. If verified, UE waits for step 7 based on the guideline received.

PHASE 2. (Service link is unavailable, Feeder link is available)

4. The satellite requests authentication data for the UE by sending the Authentication Data Request message to the ground network (GND). The request includes IMSI, SN identity, and Network type.

5. Upon the receipt of the Authentication Data Request from the satellite, HSS in the GND generates Authentication Vector(s) as defined in clause 6.3.2 in TS 33.102 [7]. Authentication Vector consists of KASME, RAND, AUTN, and XRES.

6. The GND sends an authentication response back to the satellite that contains Authentication Vector(s).

PHASE 3. (Service link is available, Feeder link is unavailable)

The satellite in this PHASE may be different from the satellite in PHASE 1.

7. The UE retries the network connection by transmitting the Attach Request.

Editor’s Note: Whether step 7 needs to be protected is FFS.

8. The satellite sends Authentication Request including AUTN and RAND.

9. At the receipt of the RAND and AUTN, the UE verifies the freshness of the received values by checking whether AUTN can be accepted as described in TS 33.102 [7]. If so, the UE computes a response RES.

10. UE responds with Authentication Response message including RES in case of successful AUTN verification. In this case, the UE computes KASME from CK, IK, and serving network's identity.

11. The satellite checks that the RES equals XRES. If so, the authentication is successful. As a result of the authentication and key agreement, an intermediate key KASME is shared between the UE and the satellite.

12. NAS SMC procedure is performed between the UE and the satellite.

### 6.25.3 Evaluation

This solution satisfies all of the potential security requirements in KI#1.

In particular, before the AKA procedure between the UE and the network is completed, the satellite and the UE check the authenticity of each other using the symmetric cryptosystem, which prevents the threats of DoS attack and false satellite attack.

To achieve this, the following changes are needed:

* eNB on a satellite generates and verifies MAC.
* UE generates and verifies MAC.

Therefore, this solution might require slightly more computational resource, but it will eliminate waste of storage resource of a satellite, which causes DoS attack captured in KI#1.

## 6.26 Solution #26: Protection of partial registration or attach accept message in S&F operation

### 6.26.1 Introduction

This solution addresses key issue #2.

### 6.26.2 Solution details

This solution proposes the protection of partial registration/attach accept message using certificate based cryptography while the UE is in possession of certificates.



Figure 6.26.2-1: Protection of partial registration/attach accept message

1. The UE is in possession of private key and certificate.

Editor’s Note: Whether the private key and certificate should be stored in ME or USIM is FFS.

1. When the service link is available (feeder link is not available), if the UE identifies that current serving cell support S&F mode and the UE is allowed to use S&F operation then UE sends Registration or Attach Request message to the AMF or MME-onboard (in satellite-1). The UE includes IMSI or SUCI in the request message. The UE additionally includes the UE’s Public key in the Certificate in the registration or Attach Request message. This Public key in the Certificate will be used to encrypt the partial registration or attach accept message.
2. The gNB or eNB and AMF or MME (onboard) are in possession (pre-configured) of the credentials to verify the UE certificate.When the gNB or eNB and AMF or MME (onboard) receives the registration or Attach Request message, it verifies the UE certificate and assigns and/or generates a Temporary Identifier for the UE.
3. As the feeder link is not available, the gNB or eNB and AMF or MME-onboard sends a NAS message as Partial registration/attach accept message to the UE. The Partial attach registration/accept message includes the generated Temporary Identifier encrypted using UE’s public key in the certificate considering the received UE’s security capability. Further, the parameters/details of the used security mechanism are included in the Partial registration/attach accept message.

Editor’s Note: How the UE verifies whether message 4 comes from a trusted party is FFS.

Editor’s Note: Potential threats (e.g., tracking) associated with using the same certificate are FFS.

1. The UE decrypts the received encrypted Partial registration/attach accept message using the private key and stores the Temporary Identifier and the received security parameters/details if any in the Partial registration/attach accept message. The UE should not trigger the registration/attach request again until paging message is received or appropriate timer value elapses.
2. When the onboard satellite-1 is connected to ground station but cannot connect to the UE i.e., the service link connectivity is unavailable and feeder link connectivity is available the AMF or MME-onboard fetches the authentication vectors, subscription details from the UDM or HSS on ground station and indicates that it is pre-fetching the subscription data without authenticating the UE.
3. The gNB or eNB and/or AMF or MME (onboard) stores the received authentication vectors, subscription details received until the service link is available.
4. When the service link is available and feeder link connectivity is not available, the on-board AMF or MME enters UE serving area and starts paging the UE with the assigned temporary identifier in the partial registration or attach accept message.
5. In response to receiving the paging message, the UE re-sends the Registration or Attach request message including the IMSI/SUCI.
6. The UE and gNB/eNB or AMF/MME-onboard performs the authentication and security procedure with the UE, once primary authentication procedure is successful, remaining steps are performed to complete the Registration or Attach procedure with the UE.
7. After successful authentication the UE and gNB/eNB and AMF/MME establishes the Access Stratum (AS), User Plane (UP) and Non-Access Stratum (NAS) security context.
8. Further message exchanges are protected using AS, UP and NAS security context appropriately

### 6.26.3 Evaluation

TBD

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

### 6.Y.1 Introduction

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

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

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

# 7 Conclusions

## 7.Z Key Issue #Z: <Key Issue Name>

Editor’s Note: This clause contains the agreed conclusions of Key Issue #Z.

Annex <A>:  
<Informative annex title for a Technical Report>

Annex <X>:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024 | SA3#115 | S3-240626 |  |  |  | Skeleton | 0.0.0 |
| 2024 | SA3#115 | S3‑240930 |  |  |  | S3-240931, S3-240932, S3-240933, S3-240934 | 0.1.0 |
| 2024 | SA3#115Adhoc | S3‑241575 |  |  |  | S3-241655, S3-241325, S3-241352, S3-241583, S3-241505, S3-241506, S3-241518, S3- 241519, S3-241530, S3-241563, S3-241581, S3-241582, S3-241589, S3-241602, S3-241603, S3-241607, S3-241609, S3-241616, S3-241627, S3-241628, S3-241629, S3-241623 | 0.2.0 |
| 2024 | SA3#116 | S3-242544 |  |  |  | S3‑242542, S3‑242637, S3‑242638, S3‑242639, S3‑242543, S3‑242642, S3‑242619, S3‑242643, S3‑242644, S3‑242645, , S3‑242627, S3‑241925, S3‑242545, S3‑242546, S3‑242161, S3‑242547, S3‑242548, S3‑242115, S3‑242114, S3‑241918, S3‑242646, S3‑242146, S3‑242550, S3‑242273 , S3‑242551, S3‑242552, S3‑242647, S3‑242648, S3‑242274, S3‑242553, S3‑242291, S3-242549 | 0.3.0 |