3GPP TR 33.777 V20.0.0 (2026-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security and privacy aspects of integrated sensing and communication (Release 20)





The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP ™ 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.

© 2026, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8

4 Architecture and security assumptions 8

5 Key issues 8
5.1 Key Issue #1: Security of sensing service authorization and sensing result exposure 8
5.1.1 Key issue details 8
5.1.2 Security threats 9
5.1.3 Potential security requirements 9
5.2 Key Issue #2: Security protection for sensing service operations 9
5.2.1 Key issue details 9
5.2.2 Security threats 9
5.2.3 Potential security requirements 9
5.3 Key issue #3 on privacy for sensing 9
5.3.1 Key issue details 9
5.3.2 Security threats 10
5.3.3 Potential security requirements 10
5.4 Key issue #4 on active attacks in sensing 10
5.4.1 Key issue details 10
5.4.2 Security threats 10
5.4.3 Potential security requirements 10
5.5 Key issue #5 on unauthorized passive sensing 10
5.5.1 Key issue details 10
5.5.2 Security threats 11
5.5.3 Potential security requirements 11

6 Solutions 11
6.0 Mapping of solutions to key issues 11
6.1 Solutions to KI#1 11
6.1.1 Solution #1.1: Authorization for sensing service request from AF 11
6.1.1.1 Introduction 11
6.1.1.2 Solution details 11
6.1.1.3 Evaluation 13
6.1.2 Solution #1.2: Authorization for Sensing Service 13
6.1.2.1 Introduction 13
6.1.2.2 Solution details 13
6.1.2.3 Evaluation 14
6.1.3 Solution #1.3: Solution on authorization for sensing service request 14
6.1.3.1 Introduction 14
6.1.3.2 Solution details 15
6.1.3.3 Evaluation 15
6.1.4 Solution #1.4: Security of the connection to the Sensing service consumer 16
6.1.4.1 Introduction 16
6.1.4.2 Solution details 16
6.1.4.3 Evaluation 16
6.1.5 Solution #1.5: authorize sensing service request using OAuth-based authorization mechanism 16
6.1.5.1 Introduction 16
6.1.5.2 Solution details 17
6.1.5.2.1 Sensing service consumer is an AF inside the trusted domain 17
6.1.5.2.2 Sensing service consumer is external AF 18
6.1.5.3 Evaluation 18

6.1.6 Solution #1.6: Sensing Service Authorization at the Sensing Function 19
6.1.6.1 Introduction 19
6.1.6.2 Solution details 19
6.1.6.3 Evaluation 20
6.1.7 Solution #1.7: Security of authorization of sensing service and sensing results exposure 20
6.1.7.1 Introduction 20
6.1.7.2 Solution details 21
6.1.7.3 Evaluation 23
6.2 Solutions to KI#2 23
6.2.1 Solution #2.1: Security for sensing service operation 23
6.2.1.1 Introduction 23
6.2.1.2 Solution details 23
6.2.1.3 Evaluation 23
6.2.2 Solution #2.2: Security of the connection between Sensing Entity and SF 23
6.2.2.1 Introduction 23
6.2.2.2 Solution details 23
6.2.2.3 Evaluation 24
6.2.3 Solution #2.3: Security protection for sensing service operations between sensing entity and SF 24
6.2.3.1 Introduction 24
6.2.3.2 Solution details 24
6.2.3.3 Evaluation 24
6.2.4 Solution #2.4: Protect communication between sensing function and entity 24
6.2.4.1 Introduction 24
6.2.4.2 Solution details 25
6.2.4.3 Evaluation 26
6.2.5 Solution #2.5: Security protection for sensing service operations between sensing entity and SF 26
6.2.5.1 Introduction 26
6.2.5.2 Solution details 26
6.2.5.3 Evaluation 26
6.3 Solutions to KI#3 27
6.3.1 Solution #3.1: Privacy by data minimization 27
6.3.1.1 Introduction 27
6.3.1.2 Solution details 27
6.3.1.3 Evaluation 27
6.3.2 Solution #3.2: Privacy by data avoidance 27
6.3.2.1 Introduction 27
6.3.2.2 Solution details 27
6.3.2.3 Evaluation 27

7 Conclusions 27
7.1 Conclusions for KI#1 27
7.2 Conclusions for KI#2 28
7.3 Conclusions for KI#3 28
7.4 Conclusions for KI#4 28
7.5 Conclusions for KI#5 28

Annex A: Change history 30

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 investigates and identifies the security threats, requirements and potential solution for Integrated Sensing and Communication (ISAC). Based on the architecture and system level enhancements studied in TR 23.700-14 [2], the work in this document focuses on the security and privacy aspects of gNB-based sensing for aerial object (e.g. drone) sensing target use cases.

The aerial object sensing target uses cases defined by TS 22.137 [3] and TR 22.837 [4] serve either the purpose of public safety, or as requested by the management entity (UAV management department, USS or UTM), without the necessity to identify the object.

Specifically, the present document covers the following:

- The identified key issues, threats, potential requirements and solutions for security protection during the service operations and procedures supporting Sensing services;
- The identified key issues, threats, potential requirements and solutions for protecting privacy for sensing data collection, sensing data processing, and sensing data exposure.

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 23.700-14: "Study on Integrated Sensing and Communication; Stage 2".

[3] 3GPP TS 22.137: "Service requirements for Integrated Sensing and Communication; Stage 1".

[4] 3GPP TR 22.837: "Feasibility Study on Integrated Sensing and Communication".

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

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[8] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[9] 3GPP TS 23.501: "System Architecture for the 5G System".

[10] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[11] IETF RFC 6083: "Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[12] 3GPP TS 23.137: " Integrated Sensing and Communication; Stage 2".

[13] IETF RFC 6455: "The WebSocket Protocol".

[14] Stefania Bartoletti, Giulia Focarelli, Ivan Palam`a, Samuele Zanini, Nicola Blefari Melazzi, Giuseppe Bianchi. "Practical Blind Full-Frame Replay Attacks on OFDM-Based ISAC Systems" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.

[15] 3GPP TR 38.765: "Study on Integrated Sensing And Communication (ISAC) for NR".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

Void.

3.3 Abbreviations

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

NOTE: The abbreviations used in this document follows the abbreviations used in TS 23.137 [12].

4 Architecture and security assumptions

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

- The architecture assumptions and principles for Integrated Sensing and Communication as defined in TR 23.700-14 [2] are used as architecture assumptions in this study.
- The security architecture, procedures, and security requirements for 5GS as defined in TS 33.501 [5] are used as a baseline.

5 Key issues

5.1 Key Issue #1: Security of sensing service authorization and sensing result exposure

5.1.1 Key issue details

In TR 23.700-14 [2], architecture for sensing services is studied to enable the 3GPP network to support sensing service invocation and revocation from the service consumer, and sensing result exposure to the service consumer.

Solutions addressing the KI#2 in TR 23.700-14 [2] of authorization and revocation for particular sensing services are developed, which focus on service request authorization or revocation based on the information of the service level agreement. Security aspects need to be discussed for the above mentioned procedures.

NOTE: Security aspects of sensing service revocation triggered by sensing service consumer is addressed in this key issue.

In addition, KI#5 in TR 23.700-14 [2] addresses the type of sensing result to be exposed and the method for the network to expose the sensing result to the service consumer. Security aspect of the exposure procedure also needs to be investigated.

This key issue is related to KI#2 and KI#5 of TR 23.700-14 [2] and addresses the security aspects for sensing service invocation, revocation, and sensing result exposure procedures between the network and sensing service consumer.

5.1.2 Security threats

Without proper authentication and authorization for sensing service, unauthorized party may be able to access to sensing service.

If the connection between sensing service consumer and NEF/SF is not protected, the attacker can tamper, inject, sniff or replay messages related to sensing service invocation, revocation and sensing result exposure.

5.1.3 Potential security requirements

The 5G system shall be able to support mutual authentication between sensing service consumer and NEF/SF.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the communication between sensing service consumer and NEF/SF.

The 5G system shall be able to authorize sensing service request from a sensing service consumer.

5.2 Key Issue #2: Security protection for sensing service operations

5.2.1 Key issue details

According to TR 23.700-14 [2], after the sensing service request from the service consumer is authorized by the network, sensing service operations will be triggered and performed by the relevant network functions, which communicate with each other to obtain the sensing result.

In TR 23.700-14 [2], there are multiple solutions proposing sensing service operation procedures supported by sensing entities and different sensing related network functions (e.g. NEF, SF). The NEF needs to discover and select the SF to trigger sensing service operation. The SF needs to select proper sensing entity to collect sensing data in a specific sensing mode. When any of the service conditions of a sensing service is no longer met, an ongoing sensing service can be revoked by the network. The security aspects of all these sensing operations and procedures are to be addressed in this key issue.

NOTE : Security aspects of service operation revocation triggered by sensing function is addressed in this key issue, as it can be viewed as one type of sensing service operations.

5.2.2 Security threats

As the sensing service operations are performed among sensing function(s) and sensing entities, if the 5GC does not support sensing service operation authorization, the sensing service operation can be abused.

If the connection between sensing entity and sensing function is not securely established, an attacker is able to tamper or inject or replay sensing control messages and sensing data, or sniff the collected sensing data.

5.2.3 Potential security requirements

The 5G system shall be able to support authorization for sensing service operations.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.

5.3 Key issue #3 on privacy for sensing

5.3.1 Key issue details

This key issue focuses on the privacy aspect of sensing.

The introduction of sensing capabilities enables the network to collect and process sensing data about objects in the public or even private environment and expose derived sensing results, all without the direct participation or awareness of the sensed object. Considering that the sensing data or sensing result can contain privacy sensitive information, the privacy aspect of sensing service needs to be investigated.

5.3.2 Security threats

If any privacy related information is contained in the sensing data and is leaked to an unauthorized party, it could lead to privacy violation.

5.3.3 Potential security requirements

The 5G system shall provide a mechanism to mitigate privacy threats in the sensing system.

NOTE: The requirement of this key issue can be addressed by mechanism out-of scope of 3GPP.

5.4 Key issue #4 on active attacks in sensing

5.4.1 Key issue details

One of the use cases for sensing technology is detection of aerial objects. In order to be useful, the result has to be reliable, i.e. report an aerial object when there is one, and report empty airspace only when the airspace is in fact empty.

During the sensing operation, an attacker could generate a radio signal that would confuse the receiving sensing node into determining that there is a aerial objects at a location where there is none (e.g. by sending a signal that exhibits the typical micro-Doppler shift typical for UAV rotors), or into determining that there is no aerial object where in fact there is one. This could be achieved, e.g. by generating noise such that the response by a real aerial object is drowned out, or perceived to come from a different location, or by echoing the sensing signal with time and doppler shift as shown in [14]. The latter attack does not require decoding or even knowledge of the sensing waveform.

NOTE 1: In TR 38.765 [15], DL NR waveform/reference signal are only used as baseline to evaluate the feasibility of sensing (i.e. evaluation assumptions), as well as the exampled values of carrier frequency, system bandwidth and numerology. Other signals and resources (e.g. RE mapping and TDD UL/DL configuration) are still up to different implementations. Whether this makes the attack less feasible is not studied in the present document.

5.4.2 Security threats

An attacker is able to mask the presence of objects or simulate presence of an object at a location, violating the desired reliability KPI and potentially leading to major consequences in the air traffic control applications.

5.4.3 Potential security requirements

The sensing system shall mitigate active attacks.

5.5 Key issue #5 on unauthorized passive sensing

5.5.1 Key issue details

The sensing mode considered in the present document is a collocated sensing transmitter and receiver. However, the sensing signal sent by the sensing transmitter is not only reflected to the collocated sensing receiver, but also attenuated and scattered in all directions. Therefore, it can be possible for an attacker to set up a sensing receiver that is not collocated with the sensing transmitter, thus allowing the attacker to perform it's own sensing. The difference with an attacker performing monostatic sensing on its own is that the attacker does not need to become active, thus minimizing the risk of being detected. In addition, the sensing transmitter of the operator's sensing infrastructure may be in a better location, i.e. higher up or closer to the target object.

NOTE 1: Unauthorized passive sensing stems from the basic fact that radiated energy can be received by third parties. Any 3GPP radio signal propagating through space, including communication signals and reference signals, can be used by an attacker. This key issue focuses on sensing signals only, and communication signals are out of the scope of this KI.

NOTE 2: The engineering feasibility to carry out this attack, e.g. to achieve the required KPI, is not studied in the present documents.

5.5.2 Security threats

An attacker may passively eavesdrop the sensing signal and infer information about aerial objects.

5.5.3 Potential security requirements

Unauthorized passive sensing should be mitigated.

6 Solutions

6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

Solutions	KI#1	KI#2	KI#3	KI#4	KI#5
#1.1	X				
#1.2	X				
#1.3	X				
#1.4	X				
#1.5	X				
#1.6	X				
#1.7	X				
#2.1		X			
#2.2		X			
#2.3		X			
#2.4		X			
#2.5		X			
#3.1			X		
#3.2			X		

6.1 Solutions to KI#1

6.1.1 Solution #1.1: Authorization for sensing service request from AF

6.1.1.1 Introduction

This solution addresses Key Issue #1: Security of authorization for sensing service invocation and revocation.

In this solution, the sensing service consumer is assumed to be an external AF. The NEF performs the access authorization by verifying the AF's identity, and the SF performs the service authorization by validating the feasibility and policy compliance of the specific sensing request parameters against network capabilities and operator rules.

6.1.1.2 Solution details

This solution proposes mutual certificate-based authentication between the NEF and the external AF/sensing service consumer using TLS. Certificate based authentication follows the profiles given in TS 33.310 [6], clause 6.1.3a. The identities in the end entity certificates is used for authentication and policy checks.

For the protection of communication between AF/sensing service consumer and NEF, TLS is used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the AF/sensing service consumer. Security profiles for TLS implementation and usage follow the provisions given in clause 6.2 of TS 33.210 [7].

After the authentication, the following procedures are used for authorizing sensing service request.

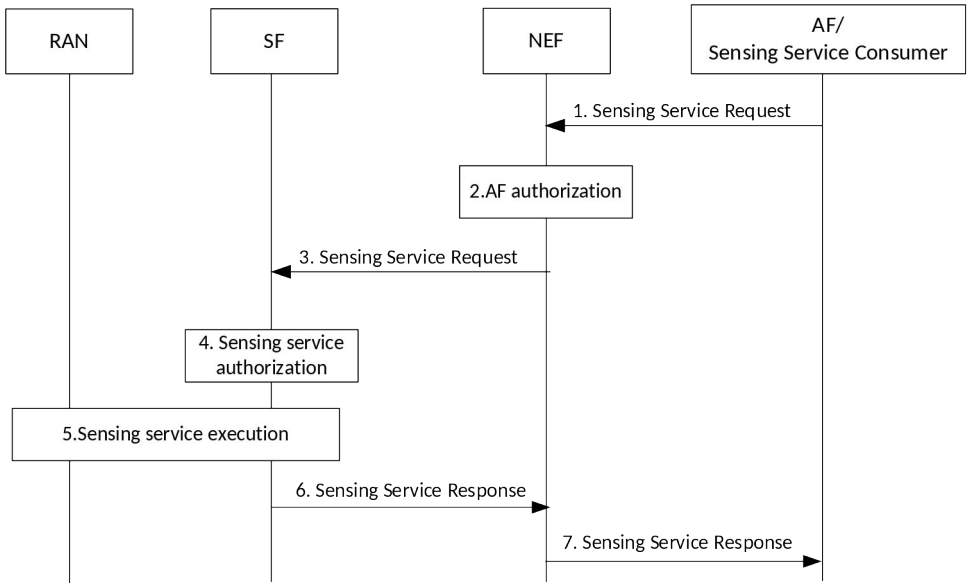


Figure 6.1.1.2-1: Procedure for sensing service authorization

1. The AF sends sensing service request message to the NEF. The message includes AF ID, OAuth 2.0 token, and sensing service related parameters (e.g. target sensing area, sensing time, sensing type, etc).

NOTE 1: Details of the sensing authorization information for sensing service are out of scope of this solution.

2. NEF performs the authorization check for the sensing service request. This includes:

- validating the OAuth 2.0 token presented by the AF; and

- checking the AF's subscription profile to verify that the AF is entitled to request the sensing service.

If the check fails, the NEF rejects the request with a failure cause.

3. If the AF is authorized by the NEF to request for sensing service, the NEF discovers and selects the SF, and sends the Sensing service request message to the SF. This message includes sensing service related parameters.

4. The SF performs sensing service authorization based on the sensing service related parameters. Specifically, this includes:

- validating the sensing service related parameters against operator-defined service policies (e.g. restricted zones, restricted time); and

- checking if the network has available resources to fulfill the request.

If the authorization fails, the SF rejects the request with a failure cause. The reject message is sent to AF via NEF.

NOTE 2: Validations performed by SF for sensing service authorization are out of scope of this solution.

5. After successful authorization, the SF proceeds to execute the sensing service.

6-7. The SF provides sensing results in sensing service response to the AF via NEF.

NOTE 3: Details of the service procedures are out of scope of this solution.

6.1.1.3 Evaluation

This solution is based on the assumption that the sensing service consumer is an external AF. This solution does not address authorization for internal AF.

This solution proposes to reuse the existing mechanism to perform mutual authentication and secure communication between sensing service consumer and NEF. Details of the OAuth framework is not addressed in this solution.

The following impacts are needed:

- NEF needs to perform the access authorization by verifying the AF's identity;
- SF needs to perform sensing service authorization.

6.1.2 Solution #1.2: Authorization for Sensing Service

6.1.2.1 Introduction

This solution addresses requirements of key issue #1.

In this solution, existing SBA security framework is reused so that authentication and communication protection among sensing service consumer and NEF/SF can be protected using existing SBA mechanism, for authorization, NRF is deemed as authorization check point, and some specific criteria for sensing, e.g. sensing service, sensing location, is considered for sensing service authorization.

6.1.2.2 Solution details

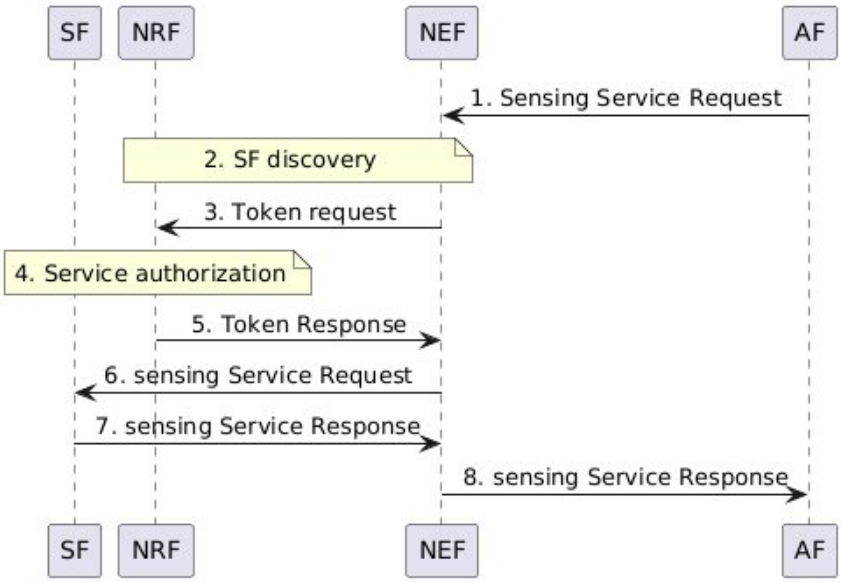


Figure 6.1.2.2-1: Authorization for Sensing Service

1. AF sends sensing service request to the NEF. The message includes the AF ID, the requested sensing services and optionally the requested sensing location for the sensing service.

2. The NEF performs SF discovery procedure via NRF.

3. The NEF sends token request the NRF as described in clause 7.1.3 of TR 23.700-14 [2].

4. The NRF performs service authorization, the NRF checks whether the AF is authorized to access the SF, whether the requested sensing services are allowed for the AF, and optionally whether the requested sensing location for the sensing service is allowed.

5. If it is authorized, NRF will issue access token and send it to the NEF, and the access token claim includes AF ID, the allowed sensing services and optionally the allowed sensing location.

6. The NEF sends sensing service request to the SF. The message includes the access token, the AF ID, the requested sensing services and optionally the requested sensing location for the sensing service.

7. After successfully verifying the access token, the SF performs sensing based on the allowed sensing services and optionally the allowed sensing location. The SF sends sensing service response including the sensing result to the NEF.

8. The NEF sends sensing service response including the sensing result to the AF.

6.1.2.3 Evaluation

The solution address authorization requirements of key issue #1.

The solution reuses existing SBA framework for token-based authorization.

According to conclusion made for static authorization in table 7.1.2-1 of TS 23.700-14 [2], AF ID, sensing area for sensing, sensing service type are criteria for authorization for sensing service, the solution proposes the similar principles for token-based authorization, those criteria will be checked by NRF and reflect on issued token.

6.1.3 Solution #1.3: Solution on authorization for sensing service request

6.1.3.1 Introduction

This solution addresses Key Issue#1 on Security of authorization for sensing service invocation and revocation. Specifically, it addresses the third requirement in KI#1: "The 5G system shall be able to authorize sensing service request from a sensing service consumer".

According to TR 23.700-14 [2], a sensing service request may be initiated by a sensing service consumer. The authorization on service permission includes two levels:

- The first level of authorization is for service access. When the NEF receives the sensing service request initiated by the sensing service consumer (e.g. an AF), the NEF can determine whether the sensing service consumer is authorized to request the sensing service from the 5GC, according to clause 12 in TS 33.501 [5].
- The second level of authorization is based on the local policy. The Sensing Function may check the Sensing Profile to verify the sensing service request from NEF to determine if a sensing service is allowed.

6.1.3.2 Solution details

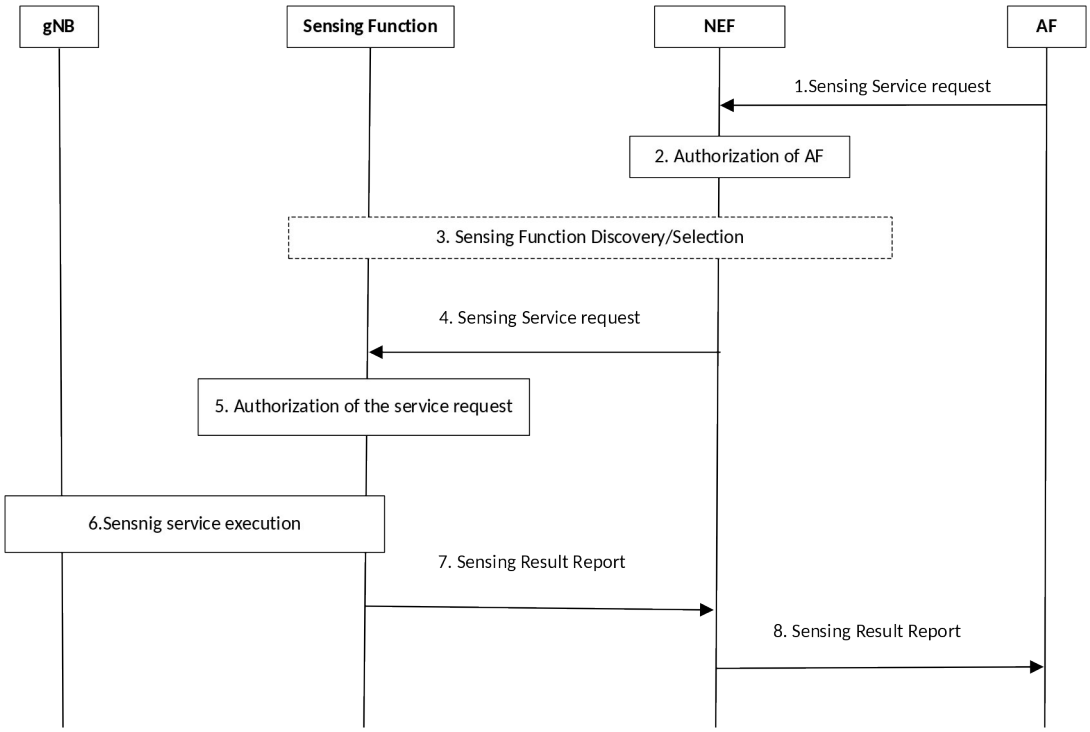


Figure 6.1.3.2-1: Authorization for sensing service request

1) The AF requests a service request for sensing. The request may include AF ID, sensing service type (object detection, object tracking, etc), sensing service requirements (e.g. accuracy, latency, etc), sensing service area.
2) The NEF may authorize the sensing service request from the AF by reusing the OAuth 2.0 mechanism in clause 12 of TS 33.501 [5].
3) The NEF may discover and select the candidate Sensing Function(s).

4) If the authorization succeeds, then the NEF sends the sensing service request message to the Sensing Function. The request message may contain AF ID, sensing service area, sensing service type, sensing service requirements.

5) The Sensing Function may authorize the sensing service request based on the local policy. The Sensing Function may check the Sensing Profiles to verify the sensing service request from NEF, which may contain allowed sensing service area, allowed sensing service type, allowed sensing service time duration, etc.

NOTE 1: The Sensing Profile is stored in Sensing authorization functionality for authorisation of the sensing service request, e.g. Sensing Function.

NOTE 2: The details of Sensing Profiles are out of scope of this solution.

6) If the authorization succeeds, then the Sensing Function proceeds to execute the sensing service.

7) The Sensing Function sends the sensing results to NEF.

8) The NEF sends the sensing results to AF.

6.1.3.3 Evaluation

This solution addresses the KI#1: "The 5G system shall be able to authorize sensing service request from a sensing service consumer".

This solution assumes that the sensing service consumer is an external AF and does not address authorization for internal AF.

This solution reuses the OAuth 2.0 mechanism defined in TS 33.501 [5] to address the authorization of AF for sensing service request in NEF.

In this solution, the authorization of AF's Sensing Service Request in Sensing Function is aligned to TS 23.700-14 [2].

No new security mechanism is introduced.

6.1.4 Solution #1.4: Security of the connection to the Sensing service consumer

6.1.4.1 Introduction

This solution aims to address the security requirements in Key Issue #1. In TR 23.700-14 [2], architecture for sensing services is studied to enable the 3GPP network to support sensing service invocation and revocation from the service consumer.

6.1.4.2 Solution details

The Sensing service consumer acts as Application Function (AF) to interact with the network. Based on the operator deployment, the Sensing service consumer can be considered as either internal AF (i.e. within operator trusted domain) or external AF (i.e. outside operator trusted domain).

If the Sensing service consumer acting as external AF then it only interacts with network via NEF. In this case the security mechanisms in clauses 12 of [5] are reused to provide mutual authentication, authorisation, integrity protection, confidentiality protection and replay protection between Sensing service consumer and the NEF.

For the Sensing service consumer acting as internal AF, it can directly access to network functions (i.e. Sensing Function (SF)). In this case the security mechanisms in clauses 13.1.0, 13.3.2.1 and 13.4 of [5] are reused to provide mutual authentication, mutual authorisation, integrity protection, confidentiality protection and replay protection between Sensing service consumer and the SF.

6.1.4.3 Evaluation

This solution addresses the security requirements of Key Issue#1, by reusing existing security mechanisms between AF and the network.

The scope of the authorisation token used in OAuth 2.0 token-based authorisation reuses the existing mechanism in clause 13.4 of [5].

6.1.5 Solution #1.5: authorize sensing service request using OAuth-based authorization mechanism

6.1.5.1 Introduction

The solution addresses KI#1 to authorize sensing service request from the sensing service consumer

Key issues related to System Architecture to Support Sensing, Authorization and Revocation to Support Sensing Service, and Sensing Result Exposure are studied in TR 23.700-14 [2]. Based on solutions for those KIs, a sensing service consumer may access sensing service from sensing function indirectly via NEF. For example, if the sensing service consumer is external AF, it accesses the sensing function through NEF. The sensing service request may trigger operation or revocation of sensing on specific object in specific area at specific accuracy level during specific time, or subscribe to specific sensing result. Sensing service authorization polices are defined in some solutions, and local policies-based authorization is also discussed in some solutions.

If the sensing service consumer is external AF, as specified in clause 12 of TS 33.501 [5], the NEF authorizes the requests from AF using OAuth-based authorization mechanism, the specific authorization mechanisms follow the provisions given in RFC 6749 [8]. When the NEF supports CAPIF for external exposure as specified in clause 6.2.5.1 in TS 23.501[9], then CAPIF core function chooses the appropriate CAPIF-2e security method as defined in the sub-clause 6.5.2 in TS 33.122[10] for mutual authentication and protection of the NEF – AF interface.

If the sensing service consumer is an AF inside the operator's domain, according to clause 13 of TS 33.501 [5] and clause 6.2.10 of TS 23.501, OAuth 2.0 based authorization is reused. Static authorization is based on local authorization policy at the SF and can be used when token-based authorization is not used.

In general, OAuth 2.0 based authorization can be reused to authorize sensing service request from sensing service consumer.

6.1.5.2 Solution details

6.1.5.2.1 Sensing service consumer is an AF inside the trusted domain

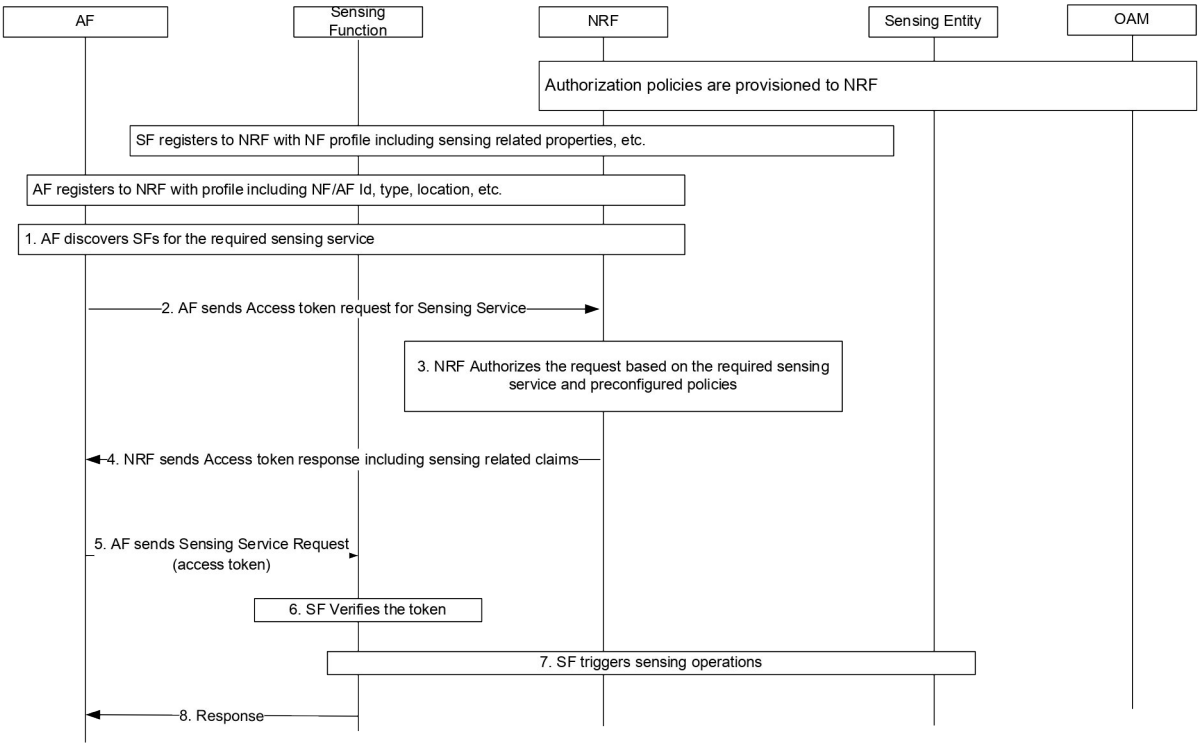


Figure 6.1.5.2.1-1

Precondition:

- OAM provisions sensing authorization policies in NRF enabling which sensing consumers are allowed to access / trigger what type of sensing operation on which kind of object in which area at which time with what level of accuracy.
- SF registers to NRF with NF profile including supporting sensing objects, sensing area, sensing accuracy, etc.
- AF registers to NRF with profile including NF/AF Id, type, location, etc.

1. AF sends request to NRF to discover potential sensing functions for the required sensing service.

2. AF sends Access token request for Sensing Service (e.g. sensing service type, sensing service area, sensing duration, sensing quality of service requirements)

3. NRF Authorizes the request based on the required sensing service, area, duration, accuracy, sensing consumer profile and preconfigured policies, etc.

4. NRF sends Access Token response including sensing related claims

5. AF sends sensing service request to a discovered SF with access token got in step 4

6-8. SF validates the token, triggers sensing operation and sends response to the AF.

6.1.5.2.2 Sensing service consumer is external AF

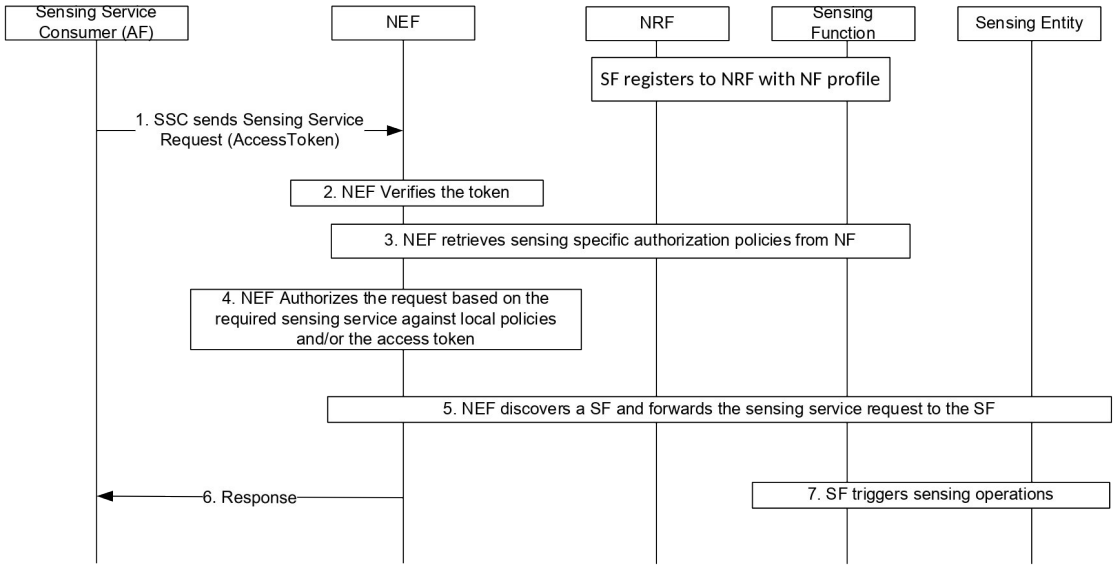


Figure 6.1.5.2.2-1

Precondition:

- OAM may provision operation access control policies and sensing authorization policies in NEF, enabling which AFs are allowed to access what type of sensing operation on which kind of object in which area at which time with what level of accuracy.
- SF registers to NRF with NF profile including supporting sensing objects, sensing area, sensing accuracy, etc.

1. SSC sends Sensing Service Request (e.g. sensing service type, sensing service area, sensing duration, sensing quality of service requirements), with the access token obtained from the Authorization Server.

NOTE 1: If CAPIF is supported, the token will be generated by CCF, which will be aware of the sensing policies.

2-4. If the information in the access token is not sufficient to authorize the request, NEF retrieves detail sensing authorization polices from other sensing specific policy function, and retrieve sensing services registered to NRF, and

authorizes the request based on the required sensing service against available sensing services got from NRF, sensing consumer information, operation access control policies and sensing authorization policies.

5-6. NEF discovers a SF based on the request and forwards the sensing service request to the SF, and sends response to the SSC.

NOTE 2: NEF follows existing discovery and authorization procedure defined in TS 23.502 and 33.501 [5] to discover and access the SF.

7. SF triggers sensing operation.

6.1.5.3 Evaluation

The solutions address the requirements of KI#1 when the AF is either external or internal. Both options leverage existing mechanisms, like mTLS for the authentication purposes, but differ on the authorization aspect:

- When the AF is internal, the solution proposes to enhance the OAuth2.0 framework to support sensing policies as part of the token scope. The impact is limited to NRF, that is required to understand sensing request and convey the respective authorization inside the scope of the token. This solution assumes that sensing policies are available at OAM.
- When the AF is external, the solution enhances NEF, which is aware of the authorization policies (either by configuration or by retrieving them from another NF) and enforce them before forwarding the request to SF. This alternative is not in line with SA2 conclusions, since NEF performs both the authorization of the sensing request and the authorization of the sensing operation.

The solutions impact, either NEF or NRF to act as authorization enforcing points to ensure that only authorized requests are allowed to SF.

6.1.6 Solution #1.6: Sensing Service Authorization at the Sensing Function

6.1.6.1 Introduction

This solution addresses the potential authorization requirement of Key Issue #1: Security of authorization for sensing service invocation and revocation:

"The 5G system shall be able to authorize sensing service request from a sensing service consumer."

It is proposed that the Sensing Function performs the authorization of the Sensing Request.

6.1.6.2 Solution details

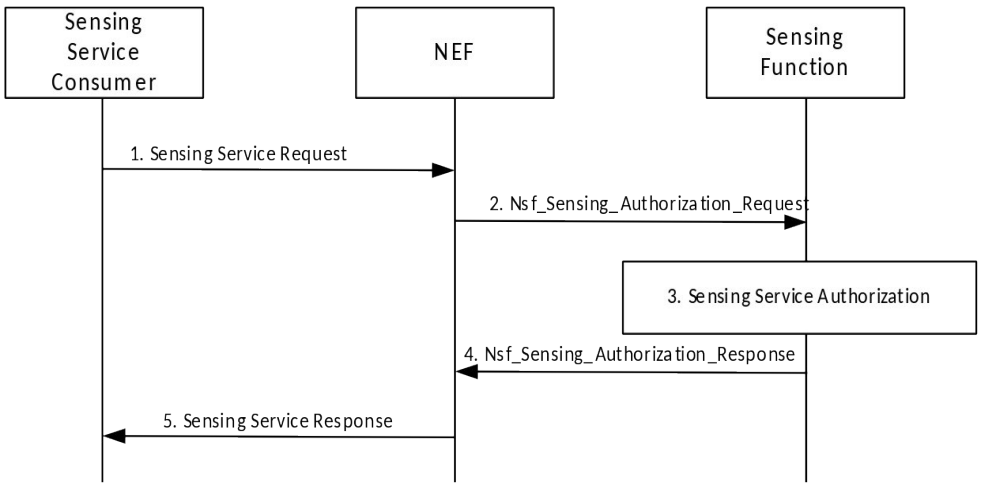


Figure 6.1.6.2-1: Sensing Service Authorization at the Sensing Function

1. It is assumed the Sensing Service Consumer (AF) and the NEF have a security association as described in TS 33.501 [5], clause 12 "Security aspects of Network Exposure Function (NEF)". The Sensing Service Consumer

sends a Sensing Service Request to the NEF with the descriptive information e.g. sensing service type (object detection, object tracking, environment sensing, etc.), sensing service requirements (e.g. accuracy, latency, resolution, etc.) and time information when the sensing service is needed (e.g. time for sensing measurement, time for sensing report) etc.

2. The NEF selects a Sensing Function for invoking the Sensing Service and to authorize the request. The NEF sends a Nsf_Sensing _Authorization_Request including the AF ID and the sensing information received from the Sensing Service Consumer to the Sensing Function.

3. The Sensing Function fetches Sensing Profile Information for the AF ID. The Sensing Function performs the authorization of the sensing request from the NEF by verifying whether the information from the Sensing Request matches the information stored in the Sensing Authorization information for the AF.

Table 6.1.6.2-1: Sensing Authorization information for Sensing Service [2]

AF Authorization Data	Description
AF ID	Identifier used to identify the AF.
Allowed/Not allowed area for sensing	Indicate the allowed/not allowed area for the indicated AF to trigger the sensing services operations (NOTE).
Allowed/Not allowed time period for sensing	Indicate the allowed time period within which AF can trigger a particular sensing service operation.
(Allowed) sensing service type	Indicate the allowed sensing service type (e.g. object tracking, detection) for the indicated AF to trigger the sensing services operations.
NOTE: The Allowed area and the Not allowed area may be both present or only one of them can be present, for example if the AF is allowed to make a request for the majority of PLMN coverage excluding the not allowed area only the not allowed area can be present. If both are not present all area is allowed.	

If the sensing service authorization is successful, the Sensing Function initiates the sensing procedure with the corresponding NF. If the sensing service authorization fails, the Sensing Function responds the failure to the NEF.

4. The Sensing Function responds to the NEF either with the sensing information result from the sensing procedure, or with a successful authorization response or with an authorization failure response.

NOTE: The messages in step 2 and step 5 is not aligned with TS 23.137 [12].

5. The NEF forwards the message from the Sensing Function to the AF.

6.1.6.3 Evaluation

This solution fulfills the potential security requirements of key issue #1:

Sensing Service Consumer (AF) authentication and authorization at the NEF as well as integrity protection, confidentiality protection and replay protection for the communication between sensing service consumer and NEF is performed according to TS 33.501 [5].

The sensing service request from a sensing service consumer is authorized by the Sensing Function according to TS 23.700-14 [2].

6.1.7 Solution #1.7: Security of authorization of sensing service and sensing results exposure

6.1.7.1 Introduction

This solution addresses the Key Issue #1 (security of sensing service authorization and sensing result exposure). Authentication, communication security, and authorization aspects for NEF and AF interaction have already been specified in Clause 12 of TS 33.501 [5]. The interface between the sensing service consumer acting as an AF and the NEF, is the same interface whose security is addressed in Clause 12 of TS 33.501 [5].

NEF sends the sensing service request to a Sensing Function (SF) after performing AF authorization. NEF and SF interaction can reuse the authentication, communication security, and authorization aspects specified in Clause 13 of TS 33.501 [5]. The SF performs authorization of the sensing service operation, considering, for instance, the received parameters for the requested sensing service (e.g. Target Sensing Area, Sensing Service Type) and information about

the sensing service consumer (e.g. AF Identifier). The SF uses the local sensing policies to perform authorization of the sensing service operation.

If authorized, the sensing service is executed, the SF provides the final sensing results to NEF. The NEF exposes the final sensing results to the authorized AF. The authentication, communication security, and authorization aspects for final sensing results exposure from NEF to AF can reuse the Clause 12 of TS 33.501 [5].

If the AF is inside the trusted domain, it can either go through via NEF or can directly interact with Sensing Function. In latter case, the internal AF can send the Sensing Service request directly to the Sensing Function. The security mechanisms in clause 13.3 of TS 33.501 [5] are reused to provide mutual authentication, authorization, integrity protection, confidentiality protection and replay protection between internal AF and Sensing Function. The SF performs a sensing request authorization using the local sensing policies, taking into account, for instance, target sensing area, AF identifier, and other parameters from the sensing service request.

6.1.7.2 Solution details

Two network entities may be involved to perform authorization of the sensing service requested by a sensing service consumer (AF) from the network. After receiving a sensing service request, NEF determines whether the sensing service consumer is authorized to invoke sensing APIs to the network. The security mechanism, specified in Clause 12 of TS 33.501 [5], is reused to address the security requirements of mutual authentication, integrity protection, confidentiality protection, replay protection, authorization for the communication between sensing service consumer and NEF.

In case the sensing service consumer is authorized to invoke sensing APIs to the network, the NEF determines parameters for the request and then sends the sensing service request to an SF. Otherwise, the NEF rejects the sensing service request due to authorization failure.

NOTE: How the NEF discovers and selects an SF to handle a specific sensing service request is outside the scope of this solution.

The security mechanism, specified in Clause 13 of TS 33.501 [5], is reused to address the security requirements of mutual authentication, integrity protection, confidentiality protection, replay protection, authorization for the communication between NEF and SF.

The SF performs a sensing request specific authorization in the implementation specific way, considering for instance, the received parameters for the requested sensing service (e.g. Target Sensing Area, Sensing Service Type, Sensing service time duration), information about the sensing service consumer (e.g. AF Identifier). The SF uses the local sensing policies to perform the sensing request authorization using the parameters of sensing request. Local sensing policies contains information about area restrictions, i.e. whether the application (based on AF Identifier) is authorized to request a sensing service in a particular area.

In case of successful authorization, the SF proceeds with the requested sensing service. If the SF determines not to grant the authorization, the sensing service request is rejected and the sensing service consumer is informed.

Procedure for a consumer-requested sensing service authorization performed by the core network entities is shown in Figure 6.1.7.2-1.

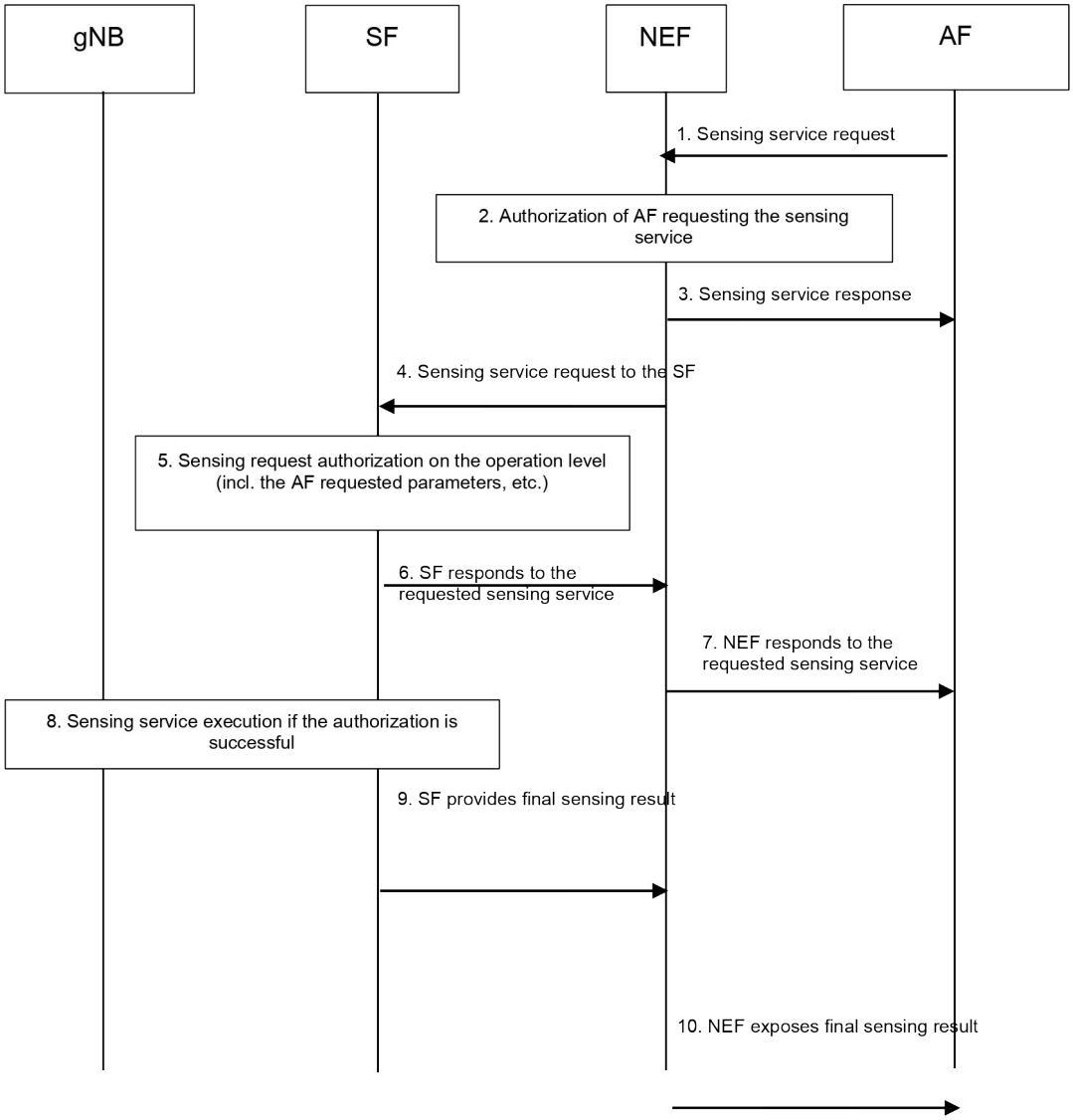


Figure 6.1.7.2-1: Procedure of the sensing service authorization and exposure

1. AF invokes a sensing service request to a NEF.

2. The NEF authenticates the AF and determines whether the AF is authorized to request sensing services from the network, i.e., to invoke sensing service-specific APIs using clause 12 of TS 33.501 [5].

3. If the authorization is not granted, the NEF sends the response to AF indicating that the authorization has failed, and all further steps are skipped.

4. If the authorization is granted, the NEF sends the sensing service request to the SF and includes parameters from the AF (e.g. Target Sensing Area, Sensing Service Type, Sensing service time duration) and information about the sensing service consumer (e.g. AF Identifier); if required, the NEF maps parameters from AF sensing service request to 3GPP internal parameters e.g. the External Target Sensing Area to a Target Sensing Area

5. The SF performs a sensing request specific authorization in the implementation specific way using the local sensing policies, considering, for instance, target sensing area, AF identifier, and other parameters from the sensing service request.

6-7. If the SF does not grant the authorization for the requested sensing service operation, the SF rejects the request and responds (via NEF) to the sensing service consumer indicating that the authorization has failed, and all further steps are skipped.

8. If the authorization is granted, the sensing service continues to provide the requested sensing result to SF.

9. SF provides the final sensing results to the NEF. The security mechanism, specified in Clause 13 of TS 33.501 [5], is reused to address the security requirements of mutual authentication, integrity protection, confidentiality protection, replay protection, authorization for the communication between SF and NEF.

10. NEF exposes the final sensing results to the AF. The security mechanism, specified in Clause 12 of TS 33.501 [5], is reused to address the security requirements of mutual authentication, integrity protection, confidentiality protection, replay protection, authorization for the communication between NEF and AF.

6.1.7.3 Evaluation

The solution addresses the security of sensing service authorization and security of sensing results exposure. It fulfils all the security requirements mentioned in Key Issue #1. In this solution the NEF performs the service access authorization of the AF for Sensing Service request and the SF performs sensing service request authorization. In this solution the Sensing Authorization information is pre-configured or configured by OAM, and stored in the SF for authorization of the Sensing Service Request. This solution only discuss local policy authorization.

6.2 Solutions to KI#2

6.2.1 Solution #2.1: Security for sensing service operation

6.2.1.1 Introduction

This solution addresses the following requirement of Key Issue #2: Security protection for sensing service operations: "*The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.*"

6.2.1.2 Solution details

The solution proposes a security mechanism to secure the connection between the sensing entity and SF.

For the interface between the sensing entities and SF, the communication between the sensing entity and the SF is secured by the NDS/IP security procedures specified in TS 33.210 [7].

6.2.1.3 Evaluation

This solution addresses the following requirement of Key Issue #2: Security protection for sensing service operations: "*The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.*"

This solution is based on the assumption that there is a direct connection between SF and sensing entity for control sensing operation and report sensing data.

This solution reuses existing mechanism to secure the communication between sensing entity and SF. No new mechanism is introduced.

6.2.2 Solution #2.2: Security of the connection between Sensing Entity and SF

6.2.2.1 Introduction

This solution aims to address Key Issue #2.

This solution to secure the connection between Sensing Entity and Sensing Function (SF). SF is responsible for to handle both sensing service control and sensing data processing.

6.2.2.2 Solution details

The SF supports a direct interface (e.g. Nx interface) to send the sensing service control signalling to sensing entity, and the sensing entity uses the same interface to reply the sensing data to the SF.

In this architecture, the integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF are offered by:

- IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of TS 33.501 [5]. IPsec is mandatory to implement on the Sensing Entity. On the SF side, a SEG may be used to terminate the IPsec tunnel.

- In addition to IPsec, DTLS is supported as specified in RFC 6083 [11]. Security profiles for DTLS implementation and usage follow the TLS profile given in clause 6.2 of TS 33.210 [7] and the certificate profile given in clause 6.1.3a of TS 33.310 [6]. The identities in the end entity certificates are used for authentication and policy checks.

6.2.2.3 Evaluation

This solution assumes the SF and sensing entity are connected via direct connection.

This solution reuses existing mechanisms to address the following security requirement: The 5G system sneeds to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.

6.2.3 Solution #2.3: Security protection for sensing service operations between sensing entity and SF

6.2.3.1 Introduction

This solution is for security protection for sensing service operations between sensing entity and Sensing Function (SF) Security.

6.2.3.2 Solution details

Security between SF (Sensing Function) and sensing entity is same as security procedures for non-service based interface security defined in clause 9 of TS 33.501 [5] using DTLS/IPsec.

Security profiles for DTLS implementation and usage follow the TLS profile given in clause 6.2 of TS 33.210 [7] and the certificate profile given in clause 6.1.3a of TS 33.310 [6].

6.2.3.3 Evaluation

This solution assumes the SF and sensing entity are connected via direct connection without AMF involvement.

This solution addresses the other security requirements of Key Issue#2 "*The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF*", by reusing existing security mechanisms of NDS/IP security of non-service based interfaces security as defined in clause 9 of TS 33.501 [5], to secure communication between sensing entity (i.e. gNB) and the Sensing Function. No new mechanism is introduced.

6.2.4 Solution #2.4: Protect communication between sensing function and entity

6.2.4.1 Introduction

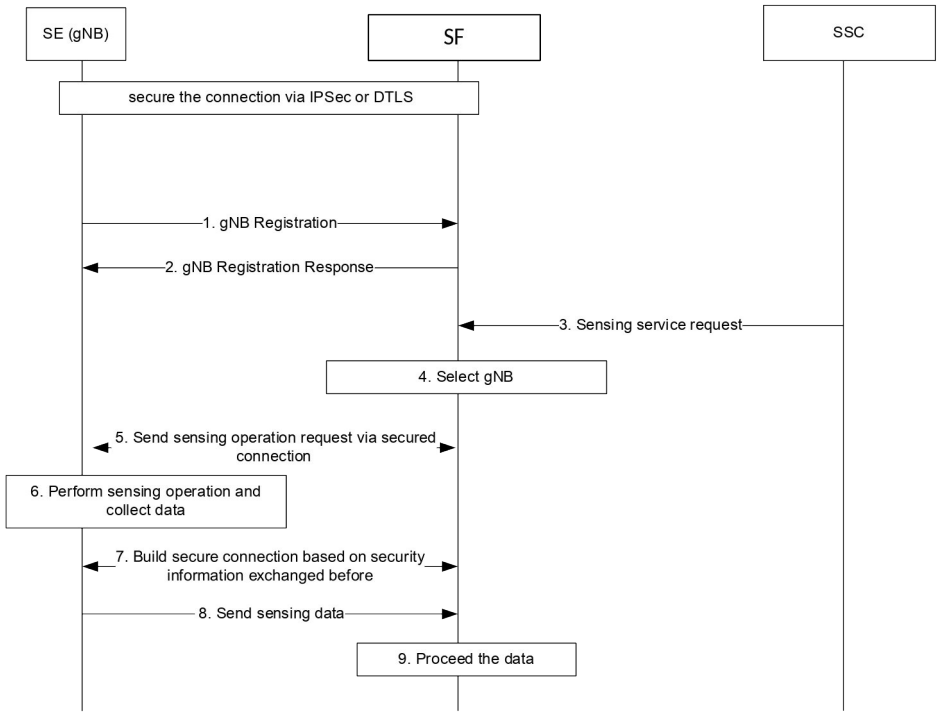
The solution addresses KI#2 to protect sensing operation and sensing data between sensing function and sensing entity.

Key issues related to System Architecture to Support Sensing, Sensing Entity Discovery and (Re-)Selection, Sensing Data and the Associated Information Collection and Transport, and Configuration of Parameters for Sensing Entities are studied in TR 23.700-14 [2]. Based on conclusion for those KIs, the sensing function and sensing entity will connect via a direct interface. The sensing entity may register its property and capability to sensing function, and the sensing function selects one or more sensing entity for sensing operation based on sensing service request and property and capability of the sensing entities. Based on configuration from the sensing function, the sensing entity will report collected sensing data. The sensing data may be included in the response of sensing operation configuration or sent in an independent report after sensing operation configuration. gNB is sensing entity in this release.

This solution proposes authentication and authorization of sensing operation configuration and sensing data reporting based on sensing architecture and procedures concluded in TR 23.700-14 [2].

6.2.4.2 Solution details

Existing mechanism defined in TS 33.501 will be reused to secure the communication between Sensing Function and Sensing Entity, mutually authenticate SF and SE, and authorize the request from SE for data reporting.



Precondition:

Existing security mechanisms, between SF and SE are re-used to establish a secure connection between SF and SE.

1. gNB registers its capabilities to SF, which include gNB profile, related properties, gNB Id, and security capabilities of the gNB.

2. Sensing function sends registration response to gNB which including Id of the SF and agreed security protocol.

3-4. After receiving sensing service request from a SSC, the sensing function selects gNB based on sensing service request and gNB profile. Additionally, SF creates a local policy based on the request, e.g. gNB1 is allowed to send drone location collected between 7 pm and 10 pm.

5. SF sends sensing operation request to the gNB.

6. gNB performs sensing operation and collect the sensing data.

7. If different connection is used to report sensing data, gNB establish secure connection towards SF.

8. After authenticating SF and built secure connection with the SF, gNB sends the sensing data to the SF via secure connection.

9. SF authorize the reporting of the sensing data against the local policies as defined in section 13.3.0 of TS 33.501 [5] and process them.

6.2.4.3 Evaluation

The solution requires SF to support local authorization, as defined in Section 13 of TS 33.501 [5] to authorize the Sensing Entity to report the data. This is in line with SA2 conclusion which states that SF should not authorize gNB as Sensing Entity.

The solution proposes to reuse existing mechanisms as defined in TS 33.501 [5] to ensure integrity protection, confidentiality protection and replay protection among Sensing Entity and Sensing Function.

6.2.5 Solution #2.5: Security protection for sensing service operations between sensing entity and SF

6.2.5.1 Introduction

This solution is for security protection for sensing service operations between Sensing Entity (SE) and Sensing Function (SF). This solution assumes that Sensing Entity and Sensing Function support a direct connection/ interface for sensing control signalling and/or sensing data reporting.

6.2.5.2 Solution details

For security protection of sensing service operations between Sensing Entity and Sensing Function, the interface between SE and SF is secured by the NDS/IP security procedures as specified in Clause 9 of TS 33.501 [5].

In order to protect the SE-SF interface reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in Clause 9.1.2 of TS 33.501 [5]. On the core network side, a Security Gateway (SEG) may be used to terminate the IPsec tunnel.

The transport of sensing control signalling and sensing data reporting over SE-SF interface is required to be integrity, confidentiality and replay-protected. The security protection of transport data depends on the underlying transport protocol used on the SE-SF interface.

If the transport layer protocol is SCTP for transport of sensing control signalling and/or sensing data reporting, then in addition to IPsec, DTLS needs to be supported as specified in RFC 6083 [11] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage need to follow the TLS profile given in clause 6.2 of TS 33.210 [7] and the certificate profile given in clause 6.1.3a of TS 33.310 [6]. In this case, existing security mechanisms for the N2 interface as specified in Clause 9.2 of TS 33.501 [5] can be reused.

If the transport layer protocol is WebSocket as specified in RFC 6455 [13] for transport of sensing control signalling and/or sensing data reporting, then in addition to IPsec, TLS needs to be supported to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for TLS implementation and usage needs to follow the TLS profile given in clause 6.2 of TS 33.210 [7] and the certificate profile given in clause 6.1.3a of TS 33.310 [6]. The WebSocket Protocol is an independent TCP-based protocol. Connection confidentiality and integrity is provided by running the WebSocket Protocol over TLS. The WebSocket server can use any client authentication mechanism available to a generic HTTP server, such as cookies, HTTP authentication, or TLS authentication.

The solution does not provide any authorization aspects/details between SE (gNB) and SF.

6.2.5.3 Evaluation

This solution reuses some of the existing mechanisms to protect non-service based interfaces. The solution addresses/fulfils the potential security requirement for key issue #2: The 5G system needs to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.

This solution is aligned with TR 23.700-14 [2], supporting that there is no need for authorisation for the gNB as the Sensing Entity, as the gNB is deployed by operator.

6.3 Solutions to KI#3

6.3.1 Solution #3.1: Privacy by data minimization

6.3.1.1 Introduction

This solution is for ensuring privacy of sensitive data in sensing results. Sensing Function should support data protection principles of minimization and purpose limitation when providing Sensing results to Sensing service Consumer.

6.3.1.2 Solution details

Sensing results should contain only the information explicitly requested by the Sensing service Consumer and authorized for exposure to the sensing service consumer. Sensing results should not include unrelated or excessive data to fulfill the request.

6.3.1.3 Evaluation

This solution ensures privacy of sensing data that is delivered to the Sensing service Consumer by performing data minimization and data filtering by removing the privacy sensitive information in sensing results. How the sensing results are filtered and how the filtering is maintained in a dynamic environment as well as whether this is filtering and maintenance of filters is feasible is out of scope of the present document.

6.3.2 Solution #3.2: Privacy by data avoidance

6.3.2.1 Introduction

This solution is for ensuring privacy of sensitive data in sensing results. The sensing service avoids sensing in areas in which privacy violations may occur

6.3.2.2 Solution details

Sensing signals are only steered into areas in which no privacy violations can occur, i.e. the sensing beamform is steered only into an area well above the ground and built environment, thus avoiding to sense persons or items that could violate privacy.

6.3.2.3 Evaluation

This solution ensures privacy of sensing data that is generated leading to minimization without having to filter data. This solution has the drawback that take off and landing of aerial objects could happen in areas that are then not covered by sensing. How the area definition and physical steering is maintained as the environment changes and whether this is feasible is out of scope of the present document.

7 Conclusions

7.1 Conclusions for KI#1

Based on the authorization mechanisms specified in TS 23.137 [12]:

- If the sensing service consumer is the third-party AF, already existing security mechanisms in clause 12 of TS 33.501 [5] are reused to provide mutual authentication, authorisation, integrity protection, confidentiality protection and replay protection between sensing service consumer and the NEF.

NOTE 1: Third-party AF, as defined in TS 33.501 [5], corresponds to the AF outside the trusted domain in section 7.2 of TR 23.700-14 [2].

- If the sensing service consumer is the internal AF (i.e. within operator trusted domain), for local policy authorization existing security mechanisms in clause 13.3 of TS 33.501 [5] are reused to provide mutual authentication, authorisation, integrity protection, confidentiality protection and replay protection between sensing service consumer and the SF.

NOTE 2: Whether and how token-based authorization mechanism is used is to be decided in normative phase.

7.2 Conclusions for KI#2

Existing security mechanisms (e.g. DTLS, IPsec) will be reused to protect the connection between sensing entity and sensing function.

NOTE 1: Which security mechanisms are reused will be decided in normative phase, depending on protocol specified in TR 38.765 [15].

NOTE 2: Authorization aspects of KI#1 and KI#2 will be discussed during normative phase.

7.3 Conclusions for KI#3

It is agreed that no solution will be specified for this key issue. The following content will be captured during the normative phase and is only for information.

Collection: For the use case of aerial object sensing, the 5GS has to minimize the collection of incidental or implicit information beyond the intended sensing purpose. It is not guaranteed that any mechanisms will effectively realize data minimization for data collection, and consequently their applicability requires careful consideration as per the risk posed.

Exposure: For the use case of aerial object sensing, sensing results contain only the information explicitly requested by the sensing service consumer and authorized for exposure to the sensing service consumer. The SF ensures that sensing results do not include data unrelated to sensing target, i.e., aerial object. If non-aerial objects are incorrectly reported as aerial objects, this can result in information related to non-aerial objects being exposed. This issue is not addressed in the present document.

7.4 Conclusions for KI#4

Active attacks on sensing functions may attempt to manipulate sensing outcomes by injecting, replaying, or modifying radio signals to generate false or misleading sensing results (e.g. false detections or false motion information). Therefore, sensing service providers need to consider the possibility of active attacks such as echo spoofing when designing and configuring their solutions and deployments.

Prevention: Implementations may employ waveform features, signaling variations, or operational diversity that reduce predictability of the sensing signal and thereby increase robustness against replay-based or deceptive attacks. The details of these countermeasures, the efficacy of these countermeasures, and the impact on the system have not been studied or discussed within the present document.

Detection: Implementations may apply internal consistency or plausibility checks on sensing results (e.g. temporal continuity, kinematic constraints, or correlation across sensing observations) to reduce the impact of implausible or inconsistent sensing results. The details of these countermeasures, the efficacy of these countermeasures, and the impact on the system have not been studied or discussed within the present document.

It is agreed that no solution will be specified for this key issue. The following content will be captured during the normative phase and is only for information.

Different kinds of active attacks can be performed to achieve sensing outcome manipulations. No prevention and detection mechanisms are specified. Due to the variety of attacks, it is not guaranteed any mechanisms will effectively protect the sensing results, and consequently their applicability requires careful consideration as per the risk posed.

7.5 Conclusions for KI#5

Passive observation of sensing signals may allow inference of sensing outcomes and cannot be prevented; implementations may consider some countermeasures as for the prevention of active attacks (see clause 7.4). The details of these countermeasures, their efficacy, and the impact on the system have not been studied or discussed within the present document.

It is agreed that no solution will be specified for this key issue. The following content will be captured during the normative phase and is only for information. Unauthorized passive sensing attacks could be possible by observation of the sensing signals and inferring the sensing outcomes. Different kinds of unauthorized passive sensing attacks could be performed. No prevention or detection mechanisms are specified. Due to the passive nature and variety of such attacks, it is not guaranteed that any mechanism will effectively mitigate unauthorized passive sensing, and consequently its applicability requires careful consideration as per the risk posed.

Annex A:
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2025-08	SA3#123	S3-252869				Skeleton for ISAC Security TR	0.0.0
2025-09	SA3#123	S3-253011				Implemented S3-252693, S3-253012, S3-253013 and S3-253014	0.1.0
2025-10	SA3#124	S3-253728				Included changes from S3-253744, S3 253856, S3-253849, S3-253850. S3-253746, S3-253747, S3-253748, S3-253851,S3-253751, S3-251750, S3-253852, S3-253357	0.2.0
2025-11	SA3#125	S3-254538				Included changes from S3-254603, S3-254750, S3-254751, S3-254604, S3-254196, S3-254605, S3-254606, S3-254249, S3-254607, S3-254608, S3-254609, S3-254610, S3-254611, S3-254612, S3-254151, S3-254613, S3-254614, S3-254615, S3-254616	0.3.0
2026-02	SA3#126	S3-260952				Included changes from S3-260951, S3-261007, S3-260968	0.4.0
2026-04	SA3#127	S3-261659				Included changes from S3-261267, S3-261814, S3-261799,S3-261268, S3-261549, S3-261660, S3-261815, S3-261662, S3-261804, S3-261663, S3-261664	0.5.0
2026-05	SA3#128	S3-262522				Included changes from S3-261978, S3-262521, S3-262523, S3-262524, S3-262525, S3-262527, S3-262528, S3-262563, S3-262565	0.6.0
2026-08	SA3#129	S3-263514				Included changes from S3-263160, S3-263432, S3-263517, S3-263518, S3-263519, S3-263520	0.7.0
2026-09	SA#113	SP-260800				Presented for information and approval	1.0.0
2026-09	SA#113					EditHelp review and upgrade to change control version	20.0.0