Satellite and Terrestrial Network for 5G

D4.5
Extending 5G Security to Satellites

Topic	ICT-07-2017
Project Title	Satellite and Terrestrial Network for 5G
Project Number	761413
Project Acronym	SaT5G
Contractual Delivery Date	13 December 2019
Actual Delivery Date	13 December 2019
Contributing WP	WP4.5
Project Start Date	1 June 2017
Project Duration	33 months
Dissemination Level	PU
Editor	TNO
Contributors	TNO, AVA

Document History			
Version	Date	Modifications	Source
0.1	06/12/2017	Initial structure	TNO
0.2	22/12/2017	Added threat and vulnerability analysis based on D2.1 and D2.2	TNO
0.3	05/01/2018	Added extension to 5G Security Architecture chapter	TNO
0.4	27/03/2018	Added prototype implementation chapter	TNO
0.5	31/05/2018	Adding trust models	TNO
0.6	25/08/2018	Adding the simulation results	TNO
0.7	06/12/2019	Completely rewritten, document presented for final review	TNO
0.8	13/12/2019	Review comments processed	TNO
1.0	20/12/2019	Final version	TNO

Contributors		
Name	Organisation	Contributions include
Sander de Kievit	TNO	Initial Editor, Version 0.6 of the deliverable
Iko Keesmaat	TNO	Final Editor, Rewrite of the document into version 0.7 of the deliverable, Processed review comments into version 0.8 of the deliverable
Simon Watts	Avanti	State-of-the-art of satellite security, Chapter 3

Table of Contents

List of Figures

List of Tables

List of Acronyms

5G HE AV	5G Home Environment Authentication Vector
5G SE AV	5G Serving Environment Authentication Vector
ACM	Adaptive Coding and Modulation
AES	Advanced Encryption Standard
AF	Application Function
AMF	Access and Mobility Function
ARPF	Authentication credential Repository and Processing Function
AS	Access Stratum
AUSF	Authentication Server Function
BAP	Backhaul Adaptation Protocol
CCM	Constant Coding and Modulation
CDN	Content delivery network
CMP	Certificate Management Protocol
CoS	Class of Service
CU	Centralized Unit
DASH	Dynamic Adaptive Streaming over HTTP
DN	Data Network
DRM	Digital Rights Management
DTH	Direct To Home
DTLS	Datagram Transport Layer Security
DU	Distributed Unit
DVB	Digital Video Broadcast
DVB-S2	Digital Video Broadcasting – Satellite – Second Generation
DVB-S2X	Digital Video Broadcasting – Satellite – Second Generation eXtension
EGMF	Exposure Governance Management Function
F1AP	F1 Application Protocol
GEO	Geostationary Earth Orbit
gNB	5G base station (informally: gNodeB)
GSMA	GSM Association
GTP	GPRS Tunnelling Protocol
GW	Gateway
HPLMN	Home PLMN
HRES	Hash RESponse
HTS	High Throughput Satellite
HTTP	Hypertext Transfer Protocol
HXRES	Hash eXpected RESponse
IAB	Integrated Access and Backhaul
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	IP Security
LAN	Local Area Network
LEO	Low Earth Orbit
MAC	Message Authentication Code
MAC	Medium Access Control
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
MnF	Management Function
MNO	Mobile Network Operator
MnS	Management Service
MPEG	Moving Pictures Experts Group

MT	Mobile Termination
N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum
NEF	Network Exposure Function
NMS	Network Management System
NR	New Radio
NTN	Non-Terrestrial Network
OSS	Operation Support System
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PDU	Protocol Data Unit
PEP	Performance Enhancing Proxy
PHY	Physical Layer
PLMN	Public Land Mobile Network
QoS	Quality of Service
RAN	Radio Access Network
RES	RESponse
RLC	Radio Link Control
RRC	Radio Resource Control
SA	Security Association
SaT5G	Satellite and Terrestrial Network for 5G
SBA	Service Based Architecture
SCPC	Single Channel Per Carrier
SCTP	Stream Control Transmission Protocol
SEAF	Security Anchor Function
SEG	Security Gateway
SEPP	Security Edge Protection Proxy,
SIDF	Subscription Identifier De-concealing Function
SIM	Subscriber Identity Module
SMF	Session Management Function
SNO	Satellite Network Operator
SSH	Secure Shell
STB	Set-Top Box
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCP	Transmission Control Protocol
TNGF	Trusted Network Gateway Function
UDM	Unified Database Management
UDP	User Datagram Protocol
UE	User Equipment
UP	User Plane data
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
vHTS	Very High Throughput Satellite
VLAN	Virtual Local Area Network
VPLMN	Visited PLMN
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WLAN	Wireless LAN
XRES	eXpected RESponse

Executive Summary

This deliverable investigates the security aspects of integrated satellite and 5G networks, focussing on the one hand on the way existing security mechanisms may complicate the usage of satellite networks and their optimizations, and on the other hand on new security mechanisms that may be needed for the integration and sharing of networks.

The work in this deliverable makes use of the architecture scenarios defined in D3.1. In particular D4.5 focusses on the following integration scenarios:

- Indirect satellite access, i.e. satellite network as transport network for backhaul and interconnection;
- Direct satellite access where satellite networks act as roaming partners for terrestrial mobile networks;
- Direct satellite access where satellite networks are integrated as another type of access network in terrestrial networks.

For the scenarios where satellite networks act as transport network the most important issue found is the common practice of terrestrial networks to protect backhaul and interconnect interface by using IPsec. This common practice interferes with the also common practice of satellite networks to deploy TCP acceleration techniques in order to overcome the higher latency of satellite connections and restricts the ability to apply class of service over the satellite link. The use of TLS instead of IPsec may be a solution.

For the scenarios where direct access to satellite networks is deployed an integration of satellite networks in many cases requires the adoption of 5G authentication procedures in the satellite network. Hence, satellite networks may have to adopt the use of USIMs in satellite terminals and the storage of secret key information in secure databases.

In many cases integration would benefit by having a secure way of integration of management systems of satellite networks with those of terrestrial networks.

The simultaneous support of satellite networks for multiple terrestrial networks could be realized by the 5G technology of network slicing. A major security requirement in that case is the isolation of individual slices, so that data carried over a satellite network for a certain terrestrial network cannot be eavesdropped or tampered with by other terrestrial networks supported by the same satellite network.

The concern that the extra delay caused by satellite networks will negatively impact the existing security procedures is found not to be necessary. The extra delay will not interfere with security protocol timers unless there is a high amount of packet loss (and hence retransmissions) at IP level.

The concern that security mechanisms put a high load on satellite connections is found also not to be necessary. Security procedures are most often based on a minimum amount of signalling and in many cases (e.g. during handover/mobility) key changes are performed locally with only minimal signalling needed to indicate the need for these changes.

A major conclusion of the investigation of security in integrated satellite and 5G networks is that there is no need for standardization in 3GPP in the area of security. There is, however, a need for closer (business) cooperation between satellite networks and terrestrial networks, and integration would benefit from ongoing integration of management systems, but this is mostly out-of-scope of 3GPP. It should also be noted that in some areas (e.g. in the area of base station relay, in the area of management system integration, and in the area of edge computing) work is still ongoing in 3GPP.

One of the interesting areas for future work can also be the use of satellite networks as trusted non-3GPP access networks. Although currently it appears that trusted non-3GPP access and untrusted non-3GPP networks deploy mostly the same techniques, the use of trusted non-3GPP access potentially offers an opportunity for closer integration between satellite networks and terrestrial networks.

1 Introduction

1.1 Document context

For the integration of satellite into 5G networks, security is considered important. On the one hand integrated networks need to be as secure as their constituent networks. Integration may also need new security mechanisms (e.g. when integrating management systems) and in case of sharing of networks there is a need to isolate the users of the shared networks. On the other hand, security mechanisms must not prevent the normal operation of networks and, for instance, should not interfere with optimizations used in satellite and 5G networks.

This deliverable investigates the security aspects of integrated satellite and 5G networks, focussing on the one hand on the way existing security mechanisms may complicate the usage of satellite networks and their optimizations, and on the other hand on new security mechanism that may be needed for the integration and sharing of networks.

In this deliverable both the state-of-the-art of security in 3GPP 5G networks and of security in satellite networks are used as guidance for the investigation. New security mechanisms are also evaluated in terms of standardization potential in 3GPP.

1.2 Relation to other Work Packages

The relation of the work in this deliverable to the work performed in other Work Packages is illustrated in the diagram depicted in Figure 1-1 below noting that this deliverable reports on the work undertaken in WP4.5 “Extending 5G security to satellites”.

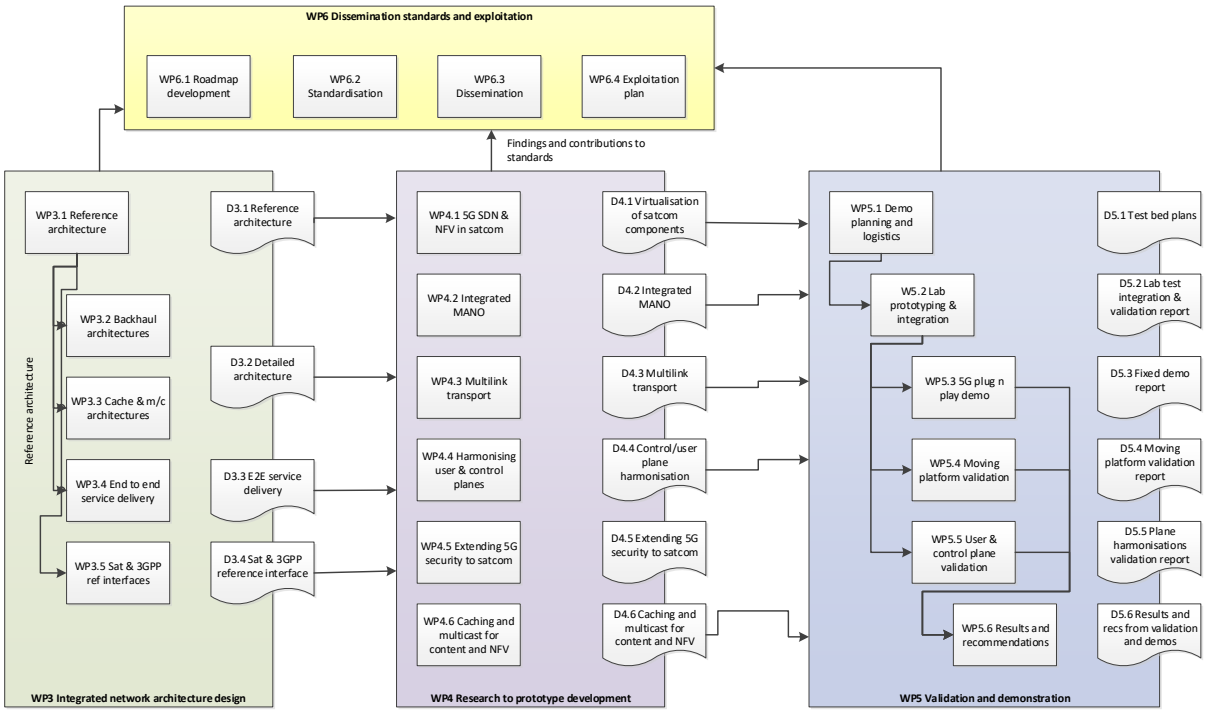

Figure 1-1: WP4 Strategy approach and SWP4.x interaction

As can be seen in Figure 1-1:

- The reference satellite network architecture described in the WP3.1 deliverable D3.1 has been used as input for the work in this deliverable;
- During the creation of this deliverable standardization potential (related to 3GPP) has been investigated. It has resulted into some related work done as part of WP6.2, i.e. writing of contributions and defending them in 3GPP meetings. The main conclusion, however, does not give rise to much standardization possibilities.

1.3 Document organization

Chapter 2 provides an overview of security mechanisms in 5G networks. It first presents the mechanism for device authentication. Then it discusses the mechanisms used in access networks for 3GPP access and for (untrusted and trusted) non-3GPP access networks. It also discusses the architecture used for base station relay (i.e. IAB – Integrated Access and Backhaul) as is currently under development in 3GPP. Security mechanisms for protecting backhaul, core network and interconnection interfaces are presented. Then it briefly discusses the security mechanisms used during handover/mobility and how privacy of the user identities is protected.

Chapter 3 presents the state-of-the-art of satellite security. It discusses areas where security of satellite backhaul might become compromised, namely in the modem, in the transmission and in the network.

Chapter 4 introduces the security threats and solutions in various integrated network scenarios. After the scenarios where satellite networks are used (both for backhaul and for interconnection), the scenarios for integration of satellite based on relay, roaming, and access network integration, respectively, are presented. The chapter concludes with security concerns for content delivery.

In chapter 5 previous information is reviewed in order to highlight complications that may arise when using existing security solutions in integrated scenarios. First the impact of using IPsec on satellite connectivity is discussed, touching the problems with TCP acceleration techniques, with QoS differentiation, and with multicast. Next the impact of using satellite connectivity on existing security solutions are discussed, touching on whether or not there is impact due to the increase in latency and touching on the impact of security solution on the load of satellite connections. Finally in this chapter the view on integration of 5G security mechanisms with satellite networks is presented.

Chapter 6 further discusses a number of new security aspects. First the need for isolation of network slice and virtual networks is treated. Then the possibilities and requirements related to integrated management and orchestration are presented. Finally, edge computing and local caching in content delivery networks and security issues in relation to multicasting are handled.

The document concludes in Chapter 7 with conclusions and considerations for future work.

2 State-of-the-art in 5G security

2.1 Overview

Security in mobile networks (including in 5G networks) always focussed on the following aspects:

- Authentication (and authorization);
- Integrity (and replay) protection; and
- Confidentiality protection.

Authentication and authorization are about verifying the identity of devices/users (in particular mobile devices) and authorizing their access to the mobile network or to particular entities in this network. Within 3GPP access by personnel to network entities is not in scope of standardization, so this aspect mainly concerns access by user devices and by other networks (e.g. via interconnection).

Integrity protection is related to protection against tampering, that is preventing the unauthorized changing of data during transmission. Replay protection is a special form of this, focussing on the unauthorized repeating of messages used to disturb the normal processes in the network.

Confidentiality protection is related to protection against eavesdropping, that is the unauthorized obtaining of data during transmission.

A fourth 'security' aspect that has gained more attention in 5G network is the protection of:

- Privacy.

Privacy protection is about protection against disclosure of user related information via which behaviour, location, and movement of users can be determined.

In order to achieve the four above-mentioned forms of security a number of dedicated network elements have been defined in 3GPP and together with an system of secret keys and derivation techniques the appropriate forms of protections can be achieved.

In the diagram depicted in Figure 2-1 (created based on information from 3GPP TS 33.501 [1] and TS 23.501 [2]) the so-called security architecture containing the relevant network entities are presented. In addition to the security related components also the relevant interfaces of 5G networks are indicated.

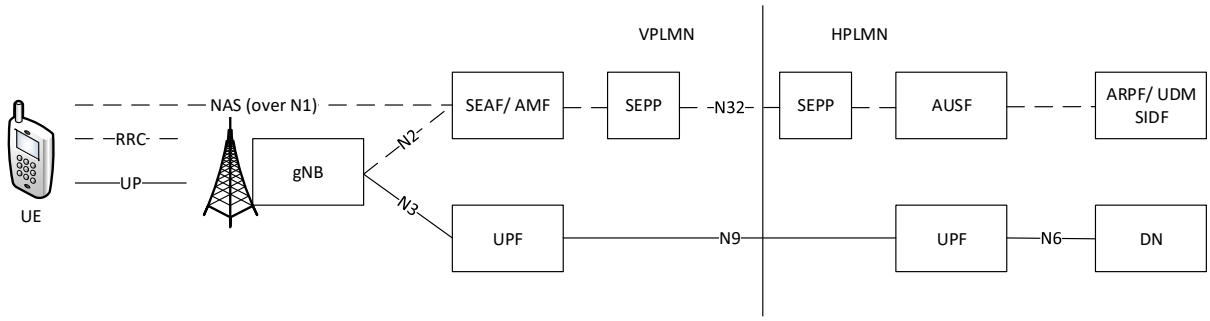

Figure 2-1: Security architecture of 5G networks

For authentication/authorization of UEs the elements SEAF, AUSF and ARPF play a role. The SEAF function is usually co-located with the AMF function, and the ARPF function is usually co-located with the UDM function. More details about this security mechanism is given in Section 2.2.

Traditionally a major part of the focus of security in mobile network is the protection of the data transmitted over the air, i.e. between UE and gNB (the 5G base stations – represented in the diagram by the box with the radio tower). Data transmitted here are

- the signalling between UE and gNB (for setting up and maintaining the radio connection) officially called radio resource control – RRC;
- the signalling between UE and the 5G core network (i.e. initially the AMF) officially called network access stratum – NAS; the interface carrying this traffic is called N1;
- user data, in the diagram denoted by user plane – UP.

More details about security mechanisms are given in Section 2.3, which is subdivided in sections related to 3GPP access, and the two forms of non-3GPP access: untrusted and trusted.

Another part of the focus of security in 5G mobile network is the protection of the data transmitted between networks of different operators, the so-called interconnection data. The most common form of this interconnection is between a visited network (VPLMN – Visited Public Land Mobile Network) and a home network (HPLMN - Home Public Land Mobile Network). For the protection of this interface pairs of SEPPs are used which protect the signalling data over this network (carried over the N32 interface). More details about security mechanisms for this interface are given in Section 2.4.3.

Security mechanisms for the other core network interface (e.g. for backhaul and internal core) are not as widely standardized as for the other interfaces (see Section 2.4.1 and Section 2.4.2).

Security during handover/mobility of a UE from one gNB to another gNB, is in scope of 3GPP and this is discussed in Section 2.5. Due to an efficient local handling of security context updates, no new messages and no new network elements are needed here.

Privacy protection in 5G network has mainly focussed on protecting the main user identity called the SUPI – Subscriber Permanent Identifier (the 5G equivalent of the IMSI in earlier generations). This identifier is representing the subscription of a user and it gives them access to the mobile network. It privacy is ensured by encryption in the UE and decryption with the help of the SIDF function (co-located in the UDM).

2.2 Authentication

At first start-up of a 5G UE, the UE and the 5G network performs a so-called primary authentication and key management. During this process the 5G UE and the 5G network authenticate each other (i.e. via mutual authentication) and a number of keys for subsequent protection are generated in the 5G UE and the 5G network.

The process of (mutual) authentication is based on secret (long-term) keys (and other parameters) stored in a USIM - Universal Subscriber Identity Module in the 5G UE, and in the ARPF in the 5G core network of the home operator (the HPLMN). It is illustrated in Figure 2-2.

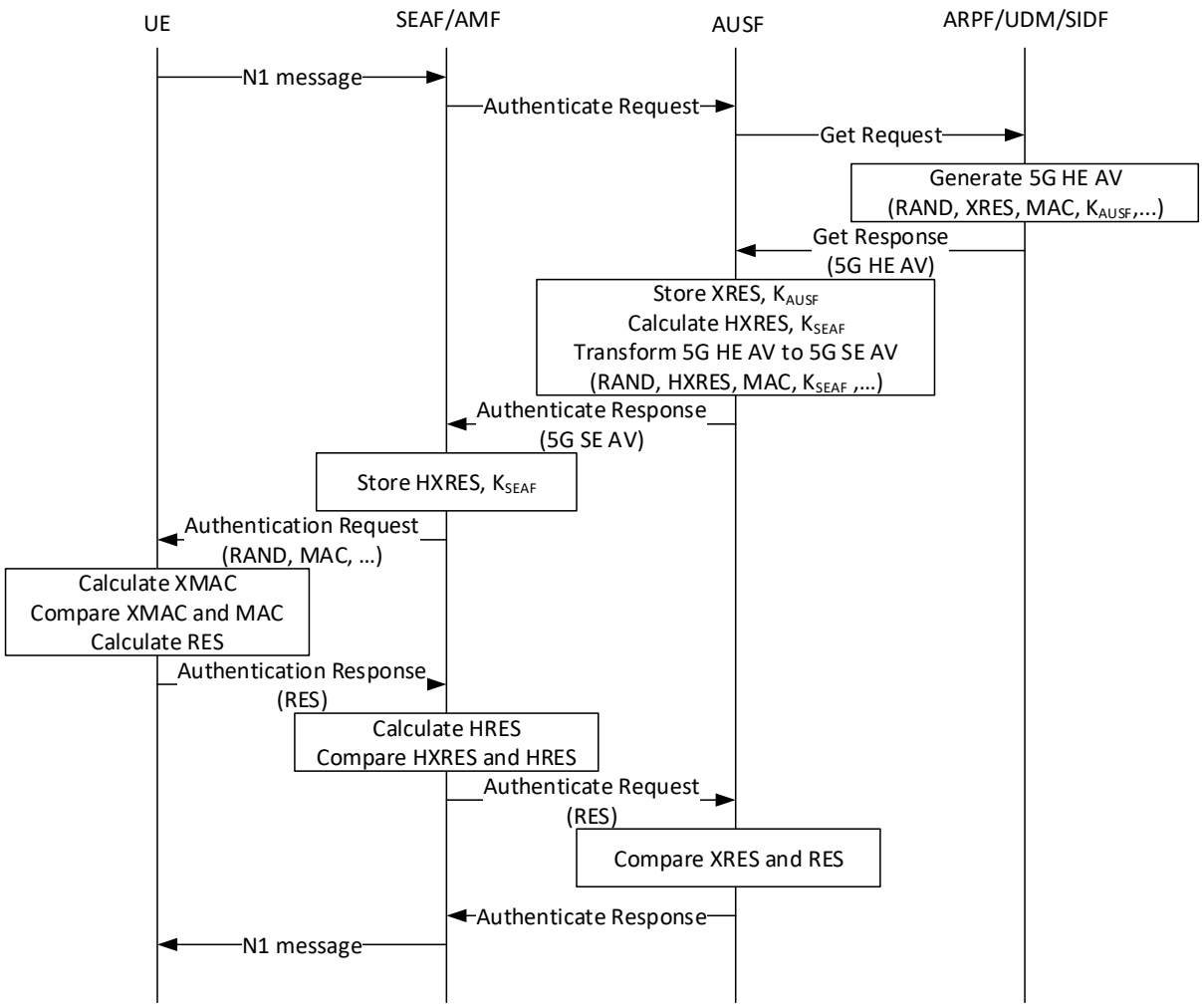

Figure 2-2: Mutual authentication based on shared secret keys

During the process of authentication, the ARPF generates a so-called authentication vector containing a random value RAND, an expected result XRES, and other information (including a so-called Message Authentication Code – MAC). In the AUSF the authentication vector is subsequently transformed and sent to the VPLMN (visited PLMN) where the included K_{SEAF} is stored (in the SEAF). In this transformed vector an expected result HXRES is included. The relevant information items of the authentication vector are then sent to the UE. After receiving these information items, the UE generates (based on its own stored secret information) an expected message authentication code XMAC and a result RES. It compares the calculated XMAC with the received MAC and thereby verifies the authenticity of the 5G core network. It then sends the calculated result RES to the VPLMN which calculate a corresponding HRES and compares this with the previously stored HXRES. If they are equal the VPLMN considers the UE authenticated and subsequently sends the RES value to the AUSF in the Home PLMN (HPLMN). Here the RES value is compared to the received XRES value and if equal the UE is considered to be fully authenticated.

In the above process it can be observed that it is ultimately the HPLMN that verifies the authenticity of the UE and not the VPLMN. This is different from the situation in previous generations and it is an indication that VPLMNs are not trusted in all respects any more.

During the authentication process described above a number of derived keys have been generated and these keys are used for establishing so-called security contexts. In general, two types of security contexts can be distinguished (see 3GPP TS 33.501 [1]):

- Non-Access Stratum (NAS) security context; this is a security context between UE and AMF;
- Access Stratum (AS) security context; this is a security context between UE and gNB.

The NAS security context is based on key K_{AMF} which is derived from the key K_{SEAF} stored in the SEAF. It is used to protect the NAS signalling between UE and AMF.

The AS security context is based on the key K_{gNB} which is derived from the key K_{AMF} stored in the AMF. It is used to protect the RRC (Radio Resource Control) signalling between UE and gNB and to protect the UP (User Plane) data between UE and gNB.

After the first authentication and key management procedure the network can perform a subsequent authentication and key management procedure. This will result in the establishment of new security contexts.

2.3 Protection in access networks

In 5G networks in general three types of (wireless) access are distinguished:

- 3GPP access (a.k.a. NR 3GPP access);
- Untrusted non-3GPP access; and
- Trusted non-3GPP access.

NR 3GPP access is access via the standard NR radio technology between a UE and a gNB as illustrated in Section 2.1.

Non-3GPP access is access via other radio technologies such as WLAN. Some versions of satellite access can also be classified as non-3GPP access. Within the category of non-3GPP access two versions are distinguished: untrusted and trusted. This distinction is primarily based on the trust view and the integration view that the 5G core network has on the non-3GPP access network and this is reflected in their architecture and procedures.

Untrusted non-3GPP access networks are considered as a kind of black box and sensitive data (such as authentication data) needs to be protected when traversing such access networks (see Section 2.3.2). In this case, the UE is expected to first get connectivity to such an access network independently from any 3GPP procedures. Only after getting access, authentication to the 5G core network can be performed.

Trusted non-3GPP access networks are considered to be 'part of' the 5G network and sensitive data (such as authentication data) can traverse such networks without additional protection (see Section 2.3.3). In this case, the UE gets connectivity via such an access network as part of the process of authentication to the 5G core network.

Traditionally 3GPP standards specify the security measures used for the protection of traffic over the radio network (especially the over-the-air part) in much detail. In this section these security measures are discussed for both the traditional NR based 3GPP access and for untrusted and trusted non-3GPP access.

2.3.1 NR 3GPP access

The control plane (i.e. signalling) traffic between UE and the radio access network (i.e. the gNB) may be protected in two ways:

- Integrity protected, i.e. it cannot be tampered with;
- Confidentiality protected, i.e. it cannot be eavesdropped.

Both types of protection concern the so-called RRC-signalling, i.e. the signalling between UE and gNB for establishing and maintaining the radio connectivity between UE and gNB. Protection is optional based on settings provided by the gNB to the UE. The protection uses the key K_{RRCint} (for integrity protection) and K_{RRCenc} (for confidentiality protection) which are derived (in gNB and in UE) from K_{gNB}.

The user plane (i.e. data) traffic between UE and the radio access network (i.e. the gNB) may be protected in two ways:

- Integrity protected, i.e. it cannot be tampered with;
- Confidentiality protected, i.e. it cannot be eavesdropped.

Protection is optional based on settings provided by the gNB to the UE. The activation of user plane protection is controlled via a user plane security policy provided by the SMF to the gNB. The protection uses the key K_{UPint} (for integrity protection) and K_{UPenc} (for confidentiality protection) which are derived (in gNB and in UE) from K_{gNB}.

2.3.2 Untrusted non-3GPP access

The untrusted non-3GPP access architecture (when using satellite as access network) is as depicted in Figure 2-3 (created based on information from 3GPP TS 23.501 [2]).

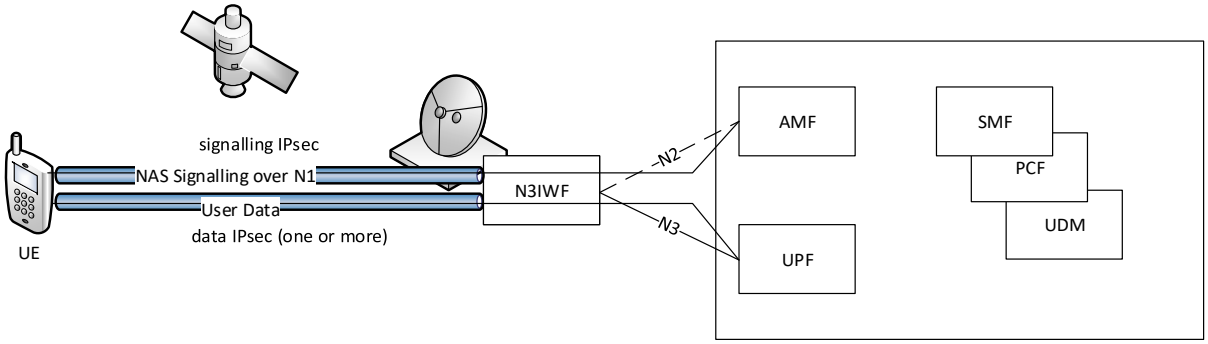

Figure 2-3: Untrusted non-3GPP access via satellite

The essential component in this architecture is the N3IWF (Non-3GPP InterWorking Function). On the one hand, this element connects to the non-3GPP access network, and on the other hand it acts as a gNB towards the 5G core network, i.e. it exposes the interfaces N2 (for signalling to the AMF) and the interface N3 (for user data to the UPF). The N3IWF also carries the UE to 5G core network NAS signalling over the N1 interface.

In case of untrusted non-3GPP access the N3IWF is required to create a number of IPsec connections to the UE and via these IPsec connections, all N1 based signalling and user data is transmitted between the UE and the 5G core network. The procedure for establishing a connection between UE and the 5G core network is performing the following steps:

- The UE is selecting an N3IWF and obtains an IP address from the N3IWF;
- The UE and the N3IWF establish a first IPsec connection, i.e. the signalling IPsec SA;
- The UE starts its authentication and registration towards the 5G core network;

After registration the UE may request subsequent PDU sessions. For these PDU sessions additional IPsec connections are created, i.e. IPsec child SAs (Security Associations). There may be more than one subsequent IPsec connections, e.g. depending on the QoS required.

As can be seen from the above IPsec is used to protect the traffic between UE and N3IWF both for NAS signalling and user data. The main IP sec SA is used for the NAS signalling and subsequent IPsec child SAs (one or more) are used for the user data. The setup of the first IPsec SA makes use of a key K_{N3IWF} which is derived from K_{AMF}.

2.3.3 Trusted non-3GPP access

The trusted non-3GPP access architecture (when using satellite as access network) is as depicted in Figure 2-4 (created based on information from 3GPP TS 23.501 [2]).

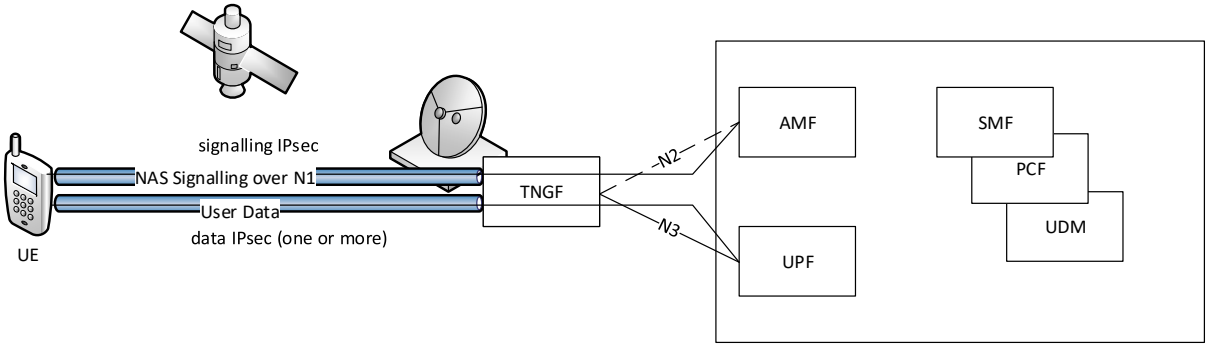

Figure 2-4: Trusted non-3GPP access via satellite

The essential component in this architecture is the TNGF (Trusted Network Gateway Function). On the one hand this element connects to the non-3GPP access network, and on the other hand it acts as a gNB towards the 5G core network, i.e. it exposes the interfaces N2 (for signalling to the AMF) and the

interface N3 (for user data to the UPF). The TNGF also carries the UE to 5G core network NAS signalling over the N1 interface.

In case of trusted non-3GPP access the TNGF will eventually create an IPsec connection to the UE and via this IPsec connection all N1 based signalling is transmitted between the UE and the 5G core network. The procedure for establishing a connection between UE and the 5G core network is performing the following steps:

- The UE selects a PLMN based on information provided by the non-3GPP access and it selects the corresponding TNGF;
- The UE starts its authentication and registration over layer 2 protocols towards the 5G core network and eventually it obtains an IP address from the 5G core network;
- The UE and the TNGF establish an IPsec connection, i.e. the signalling IPsec SA; this IPsec connection can have a null encryption and is then only used for encapsulating NAS signalling messages.

After registration the UE may request subsequent PDU sessions. For these PDU sessions additional IPsec connections are created, i.e. IPsec child SAs. There may be more than one subsequent IPsec connections, e.g. depending on the QoS required.

As can be seen from the above IPsec is used to carry the traffic between UE and TNGF both for NAS signalling and user data. The main IPsec SA is used for the NAS signalling and subsequent IPsec child SAs (one or more) are used for the user data. The impact of using trusted non-3GPP access network architectures and functionality for the integration of satellite network into 5G networks is not yet fully clear (as trusted non-3GPP access has only recently – 2019 – become specified in 3GPP), and hence needs further study.

2.3.4 Integrated Access and Backhaul

As part of the architecture work in SaT5G (see [3]), the so-called gNB relay architecture has been investigated as a way to provide tight integration between satellite networks and backhaul in terrestrial networks. In 3GPP terms, this relay architecture has been named Integrated Access and Backhaul (IAB). During the study of this concept, a number of architecture options have been investigated by 3GPP. Eventually, the (high level) architecture depicted in Figure 2-5 has been chosen by 3GPP for the support of the gNB relay functionality (in TR 38.874 [4]).

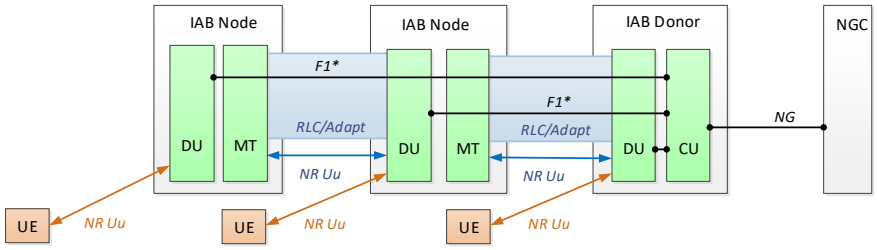

Figure 2-5: Integrated Access and Backhaul (IAB) architecture chosen as result of study (TR 38.874)

In this architecture the DU-CU split of gNBs is used to support IAB. A UE will connect (over the NR Uu interface) to the DU side of an IAB node which is controlled/connected to the CU side in the IAB donor (via modified versions of the F1-U and F1-C interfaces). The (wireless) connection between an IAB node and the next node (IAB node or IAB donor) is supported by kind of UE – gNB connection (i.e. an MT to DU connection) over its own NR Uu interface. This (wireless) connection carries the previously mentioned F1-C and F1-U traffic.

The corresponding protocol stacks, from 3GPP TS 38.300 [5] (under development), are as depicted in Figure 2-6, Figure 2-7, and Figure 2-8 respectively. In this diagrams it can be seen how the IAB architecture is a mixture of the use of the DU-CU interface (carrying the F1 protocols), which is a gNB internal interface, and the use of the NR Uu interface which is the UE to gNB interface. In contrast to the ideas expressed in SaT5G D3.1 [3] (which is based on a non-chosen architecture alternative in TR 38.874 [4]) there is not a clear separation between UE and gNB in this chosen architecture.

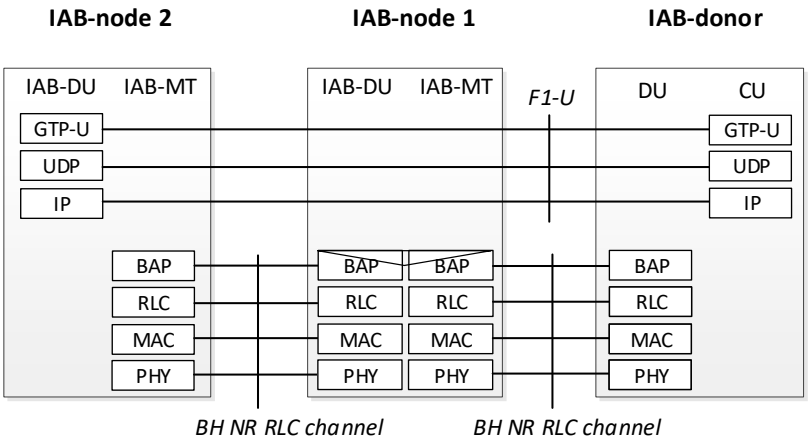

Figure 2-6: Protocol stack for the support of (modified) F1-U protocol

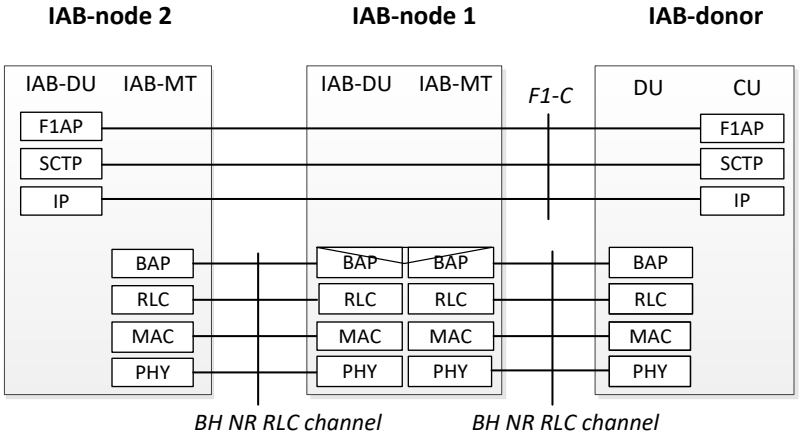

Figure 2-7: Protocol stack for the support of (modified) F1-C protocol

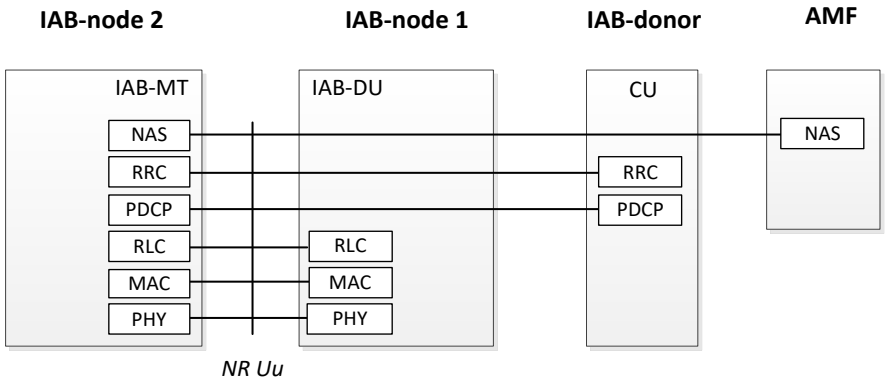

Figure 2-8: Protocol stack for the support of IAB-MT's RRC and NAS connections

Security for the IAB is currently under study in 3GPP SA3 (see 3GPP TR 33.824 [6])

2.4 Protection in backhaul, core network and interconnect networks

2.4.1 Backhaul

The backhaul connection between gNB and 5G core network consists of both the signalling (Control Plane) interface N2 between gNB and AMF and the data (User Plane) interface N2 between gNB and UPF. The same two interfaces are also used between N3IWF and 5G core network and between TNGF and 5G core network.

For the N2 interface the 3GPP standards (TS 33.501 [1]) states the following:

- The Control Plane data over N2 shall be integrity, confidentiality, and replay protected;
- It is mandatory for the gNB to support IPsec;
- On the core network side, a Security Gateway (SEG) may be used to terminate the IPsec tunnel.
- It is mandatory to support DTLS (Datagram Transport Layer Security);
- The use of cryptographic solutions to protect N2 is an operator's decision.

So, although it strongly suggested to use IPsec (or DTLS) to protect the N2 interface, it is not mandatory. It is up to the operator to use it. In practice, this means that often operators decide to use IPsec over the backhaul.

For the N3 interface the 3GPP standards (TS 33.501 [1]) states the following:

- The User Plane data over N3 shall be integrity, confidentiality, and replay protected;
- It is mandatory for the gNB to support IPsec;
- On the core network side, a Security Gateway (SEG) may be used to terminate the IPsec tunnel.
- The use of cryptographic solutions to protect N2 is an operator's decision.

So again, although it strongly suggested to use IPsec to protect the N3 interface, it is not mandatory. It is up to the operator to use it. In practice, this means that often operators decide to use IPsec over the backhaul.

2.4.2 Core network

Security mechanisms for the interface internal to an operator are usually not specified, but IPsec is suggested as a possible mechanism. Security mechanisms are only assumed if traffic crosses trust boundaries (between trust zones).

Since the NEF (Network Exposure Function) is interfacing with AF (Application Functions) outside of the operator's domain, there are security requirements on the interface between NEF and AFs: the interface shall be integrity protected, replay protected, and confidentiality protected. Moreover, the AF and the NEF shall be mutually authenticated. There are also restrictions on certain data elements that are not allowed to be sent to an AF, e.g. the SUPI (subscriber permanent identifier). And the NEF shall authorize with which network functions an AF is allowed to interact.

2.4.3 Interconnection

Control Plane security between two interconnecting networks, e.g. between VPLMN and HPLMN, is arranged via the use of the so-called SEPPs (Security Edge Protection Proxies). Each network has its own SEPP and they interconnect with each other over intermediate networks.

The SEPPs are required to protect (integrity and/or confidentiality) certain message elements. The SEPPs are required to provide integrity protection to all message elements, but they are not required to provide confidentiality protection to all message elements. The protocols needed to provide this protection are not specified, but they are assumed to be standard security protocols.

Intermediate nodes (of intermediate – carrier – networks) may be allowed to add, delete, and modify certain message elements, e.g. elements needed for routing by intermediate nodes.

When and how to protect User Plane traffic over interconnection interfaces is currently under development in 3GPP SA3: it has been studied in 3GPP TR 33.855 [7] which has led to a new work item focussing on the addition of a so-called User Plane Gateway Function (between UPFs connected via an N9 interface) in 3GPP TS 33.501 [1].

2.5 Security handling of handover/mobility

During handover of the radio connection from one gNB to another gNB new K_{gNB} values will be used by both the UE and the gNBs. The change of keys is signalled during the handover signalling, but in general no key exchange is needed between UE and gNB. The new keys are locally generated based on the old key values.

2.6 Privacy protection

The 5G equivalent of the 4G IMSI (International Mobile Subscriber Identity) is the SUPI (Subscription Permanent Identifier). These identifiers (which are stored on the USIM in a mobile device) identify the subscription of users and they are used to authenticate and authorize UEs for access to a mobile network. New in 5G is that the sending of the SUPI from the UE to the 5G network shall be protected due to privacy requirements.

In order to be able to send the SUPI, a public key shall be provided from the 5G network to the 5G UE and this shall be stored on the USIM. This key is then used to generate an encrypted identifier, the so-called SUCI (Subscription Concealed Identifier). In the 5G core network (in the UDM) this SUCI is then decrypted into the SUPI via the functions SIDF (Subscription Identifier De-concealing Function).

3 State-of-the-art in satellite security

3.1 Overview

There are a number of places where the security of a satellite communications link providing satellite backhaul services might be compromised:

- **Modem:** At the satellite modem either by access to the control mechanisms or by connecting a non-authorised modem;
- **Transmission:** Over the satellite transmission link;
- **Network:** Between the satellite transmission link and the 5G core network.

Two other attack vectors can be conceived – from the remote end RAN and directly via the satellite. The former is considered from the satcom modem perspective and the latter, albeit briefly, under network security.

This chapter provides a short review that considers primarily the traditional VSAT market that uses a variety of multiple access technologies to share radio resources. There are also point-to-point modems that use dedicated carriers in both directions, these are generally less sophisticated in their IP implementations; they use a single channel per carrier and are commonly referred to as SCPC modems.

3.2 Modem security

3.2.1 Authentication

All VSAT modems are authenticated by the VSAT hub at the satellite gateway as part of their commissioning process. This may involve the knowledge of a hardware key in the modem or use of X509 terminal authentication with enrolment certificate using Certificate Management Protocol (CMPv2) (for example see the Gilat datasheet [8] or Newtec's article [9]).

Once the VSAT hub authenticates the VSAT modem it is connected to the correct VLANs, its class of service table and IP addressing is defined. This method prevents someone from acquiring a modem, say from eBay or similar sources, and connecting to an unauthorised network.

SCPC modems often employ simpler authentication processes – as simple as a phone call between operators at each of the link.

3.2.2 Control access

SCPC modems typically use a separate LAN port for their control interface and no access to this is provided from the end user's data path.

VSAT modems often have a simple management web page that provides the end user visibility of the modem status such as radio signal levels and LAN status. It may also include a basic connectivity test option. This may be protected by a simple username and password depending on vendor implementation and SNO preference and can often be disabled; which is recommended for those providing backhaul services to public networks. Other TCP ports may also be open for specific purposes such as SSH access. These are generally disabled except in specific private network applications.

Direct access to these features is only available from the VSAT end of the link, not the VSAT hub end where the only access is via the management systems that are not connected to the user data paths.

3.3 Transmission security

The forward link from gateway to remote terminal is typically transmitted down from the satellite at fairly high power to allow the smaller antenna to receive the signal efficiently. For VSAT services this may well be modulated in DVB-S2 [10] or DVB-S2X [11] waveforms, SCPC modems may also use proprietary but similar waveforms optimised for specific purposes. These carriers often use adaptive coding and modulation (ACM) to maximise both service availability and total data throughput; others may use constant coding and modulation (CCM). Where ACM is employed this makes it difficult for a third party to snoop data from the carrier as it would need to track the modcods without having any information to do so. This adds a level of inherent security.

Most VSAT systems encrypt the unicast data on the forward link using, for example [12], 256-bit AES encryption. Some but not all systems also allow this encryption on multicast data, however such data generally has its own application layer encryption.

The return links from remote terminal to gateway are transmitted at lower power as the gateway antenna is usually sufficiently large. VSAT terminals generally send their data in short bursts against a VSAT hub managed time-plan using vendor proprietary waveforms. When using HTS satellites the downlink from the satellite will be in gateway frequency bands not user band. All this makes the return link inherently somewhat secure.

Many VSAT systems also have the option to encrypt data on the return link using the same 256-bit AES encryption algorithms. When this is implemented it may be possible to supply the VSAT system's AES encryption with a third party provided key allowing, for example, MNOs to manage the end-to-end encryption keys and relying on the VSAT system's encryption capabilities. This allows the (a) VSAT system to have visibility of the data headers to provide performance enhancement and CoS management to maximise the end users' quality of experience; and (b) the MNO to manage end-to-end security.

SCPC modems may also allow end-to-end encryption, often as a cost option.

3.4 Network security

3.4.1 Physical access to the gateway

Whilst this will be SNO specific most will follow industry standard processes such as controlling access to the site, restricting access to the data centre where the VSAT hubs and IP connections are to a restricted number of accredited and trained SNO personnel.

3.4.2 Access to the network management systems

The VSAT and IP systems will be controlled by a variety of network management systems. These will be accessed via management LANs. Access to these LANs will be controlled, for example as follows:

- Access restricted to specific internal organisation IP addresses and well-defined TCP/UDP ports;
    - These may be within the corporate WAN or by remote VPN connections;
- All accesses and system changes being logged;
- Management data exported to reporting servers that then onward link to the OSS on another secure LAN;
- Many other good practises including intrusion detection, password management processes and so forth.

All these steps are designed to make access to these management systems has hard as reasonably possible by any non-authorised person.

3.4.3 Access to the satellite

Almost all modern communication satellites operate as a bent-pipe (also referred to as transparent) because they simply receive the signal from the ground, re-transmit it without demodulating the signal, and thereby have no access to the user data nor have any access to the VSAT system control plane[1]. Therefore, no direct access to the data at the satellite is possible.

Future options for regenerative payloads – perhaps with some onboard switching – are envisaged. One example of this could be a LEO satellite-based NR RAN. These are currently still "on the drawing board" and are beyond today's state of the art and consideration in this chapter.

The spacecraft platform needs to be controlled from the ground. For example, GEO satellites need to employ station keeping to maintain their position in the correct orbital slot or perhaps to move to a new slot, also to move steerable beams as the SNO needs. Similarly, non-GSO satellites need to maintain themselves in the correct orbital plane, may need to modify orbit to avoid debris, and will need to be de-orbited at their end of life. These controls are carefully managed from secure computers (often

[1] Future vHTS systems may need to coordinate burst timing between the spacecraft and the VSATs to provide capacity flexibility implying a limited amount of control plane interaction between the VSAT system and satellite payload.

disconnected from the Internet) using various secure protocols to multiple checks before the satellite executes the commands. These measures mean the possibility of data being lost due to nefarious actions is minimised.

4 Security in integrated satellite/terrestrial 5G networks scenarios

4.1 Security aspects of satellite connections as transport network for backhaul

The scenario for satellite connections as transport network for backhaul is depicted in Figure 4-1 (created based on information from 3GPP TS 23.501 [2] and SaT5G D3.1 [3]).

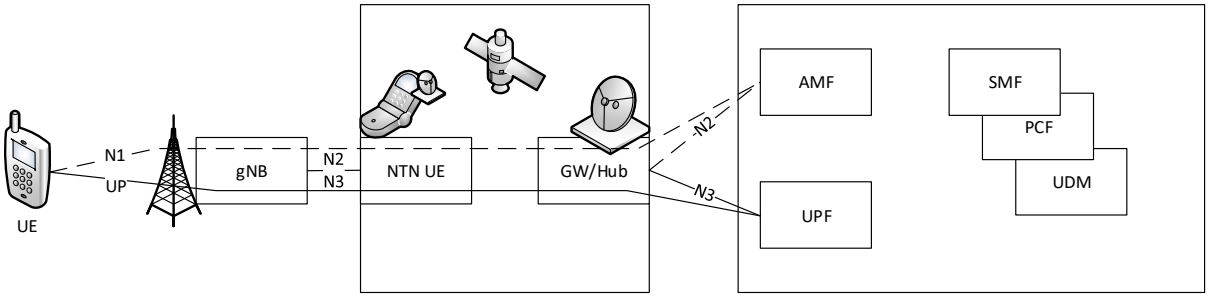

Figure 4-1: Satellite connections as transport network for backhaul

In this scenario the connections between gNB and 5G core network (in particular AMF and UPF) are provided by a satellite network composed of an NTN (non-terrestrial network) UE, (one or more) satellites, and a ground station containing a GW (gateway)/Hub. The satellite network in this case provides only IP connectivity and as such this network is transparent for the operator using the gNBs and the 5G core network.

As can be seen from the diagram four types of traffic are carried over the satellite network:

- N1 traffic, i.e. NAS signalling between UE and AMF (and onwards to SMF);
- N2 traffic, i.e. signalling traffic between gNB and AMF; this traffic includes gNB to AMF signalling (e.g. setup of the N2 link) and signalling traffic from UE to AMF (i.e. N1 NAS signalling);'
- User Plane (UP) traffic between UE and UPF;
- N3 traffic, i.e. data traffic between gNB and UPF, i.e. data traffic from UE to UPF.

Security threats and requirements

The security threats and requirements of this scenario further depend on the following aspects:

- What is the trust model between the satellite operator and the terrestrial network (consisting of the gNB and the 5G core network)?
- How many terrestrial networks are making use of the same satellite network?
- Are the management systems of the terrestrial network and the satellite network integrated or not?

A major threat perceived by terrestrial networks is the tampering and eavesdropping of traffic carried over the backhaul connection. For that reason, they require integrity and confidentiality protection of this traffic (both for control plane and for user plane traffic).

Another threat perceived by terrestrial networks in case of sharing of the satellite network is the tampering and eavesdropping of traffic via the shared network.

In case of integrated management, there is a threat of unauthorized access to the management system by the other network and/or the other management system.

Existing security mechanisms

Terrestrial networks can deploy IPsec connections between gNB and 5G core network, possibly making use of a SEG in the 5G core network. These networks may deploy a single IPsec connection for signalling and data traffic, or they may deploy multiple IPsec connections, e.g. one for signalling and one or more for data traffic (possibly grouped per QoS flow). As an alternative for the IPsec connection for signalling also a DTLS connection can be used (although this is used not very much).

Satellite networks can deploy subdivision techniques[2] (e.g. network slicing in a 5G type of network) in order to separate the usage of the network by multiple terrestrial networks. The subdivision provides isolation and resource handling, so that a) terrestrial networks are not able to access data carried by other terrestrial networks and b) each terrestrial network obtains the agreed capacity from the satellite network.

In case of integrated management the access to management systems by other entities can be controlled by the use of 'management exposure functions'. The specification of such exposure functions is only rudimentarily described in 3GPP SA5 specifications. Without this type of standardized access control functions security shall either be omitted (leading to a less secure way of working), or it shall be based on proprietary implementations.

4.2 Security aspects of satellite connections as transport network for interconnection

The scenario for satellite connections as transport network for backhaul is depicted in Figure 4-2 (created based on information from 3GPP TS 23.501 [2] and 3GPP TS 33.501 [1]).

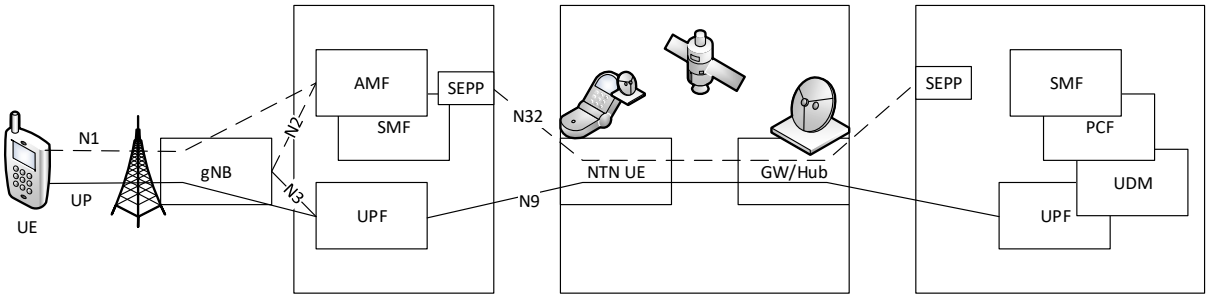

Figure 4-2: Satellite connections as transport network for interconnection

In this scenario the connections between two (terrestrial) networks (e.g. a VPLMN containing the gNB, AMF, SMF, UPF, and a HPLMN containing SMF, UDM, UPF, PCF, etc.) are provided by a satellite network composed of an NTN (non-terrestrial network) UE, (one or more) satellites, and a ground station containing a GW (gateway)/Hub. The satellite network in this case provides only IP connectivity and as such this network is transparent for the two (terrestrial) networks.

As can be seen from the diagram two types of traffic are carried over the satellite network:

- N32 traffic, i.e. SBA (service-based architecture) based signalling traffic;
- N9 traffic, i.e. data traffic between the interconnected networks.

Security threats and requirements

In this scenario the two (terrestrial) networks usually are not in the same trust domain and also the intermediate (satellite) network is not considered to be part of the trust domain of either of the two (terrestrial) networks. It is also very common to expect the intermediate to be shared among multiple (terrestrial) networks. On the other hand, it is very uncommon to expect any form of integrated management between the networks.

Since 5G the interconnection between networks is no longer fully trusted, which has caused the definition of the SEPPs in 3GPP specifications. The security threats perceived by the terrestrial network are tampering, eavesdropping, and unauthorized redirecting of traffic (i.e. traffic 'hijacking'). Initially the main perceived threat concerned the signalling traffic over the N32 interface, but recently also attention is given in GSMA and 3GPP to the threat on the user data (over N9).

Existing security mechanisms

Security mechanisms guiding the behaviour of the SEPPs is described in 3GPP specifications (see also Section 2.4.3). From these specifications, it can be seen that some data needs to be protected against eavesdropping, and other can be more freely transported. A monolithic use of IPsec between SEPP is therefore not to be expected, but some form of encryption is still required.

[2] These techniques include, for example, 802.11q based VLAN separation.

Which mechanisms are required for the protection of user data is still under development in 3GPP. It has been studied in 3GPP TR 33.855 [7], which has led to a new work item focussing on a adding a so-called User Plane Gateway Function (between UPFs connected via an N9 interface) to 3GPP TS 33.501 [1].

4.3 Security aspects of satellite connections for gNB relay

Using satellite connections to support the gNB relay node architecture (see Section 2.3.4) can be done in roughly two ways:

- Satellite network as transport network carrying the wireless connectivity between IAB-node and upstream IAB-node/IAB-donor, or
- Satellite connectivity integrated in the IAB-node and the IAB-donor.

The first sub-scenario is depicted in Figure 4-3 (created based on information from 3GPP TR 38.874 [4] and SaT5G D3.1 [3]).

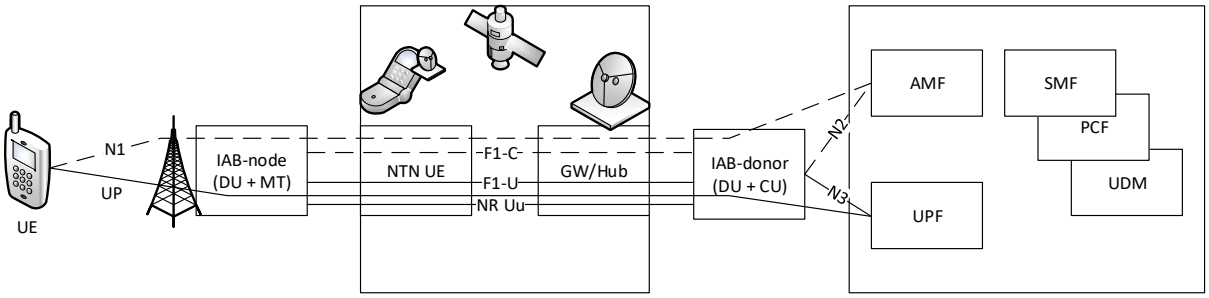

Figure 4-3: Satellite network as transport network in the IAB architecture

The second sub-scenario would require the integration of the NTN UE functionality in the IAB-node and the satellite GW/Hub functionality in the IAB-donor. In this sub-scenario the satellite connection would be required to support NR.

Integrating a satellite network operating in untrusted and/or trusted non-3GPP access mode would be quite challenging since those network models assume the N3IWF (untrusted non-3GPP access) and/or TNGF (trusted non-3GPP access) to act as a full gNB (including DU and CU) and the IAB architecture requires that they also act as gNB-CU towards the IAB-node. The latter would be hard to integrate in the non-3GPP access model.

For the first sub-scenario the security threats and requirements are very similar to the ones described for satellite as transport network for backhaul.

For the second sub-scenario it is very likely that the satellite network can be considered trusted and has integrated management. It is unlikely that the satellite network in this scenario is shared by multiple terrestrial networks.

Existing security mechanisms

There are currently no existing security mechanisms for this scenario as the security mechanisms for this scenario are currently under study in 3GPP. Usage of IPsec for the connection between IAB-node and IAB-donor is a possibility but seems not very likely as it would impose quite a lot of overhead to an interface with high performance and strict delay demands.

4.4 Security aspects of satellite networks as roaming partners of terrestrial networks

The scenario for a satellite network acting as a roaming partner to other (terrestrial) networks is depicted in Figure 4-4.

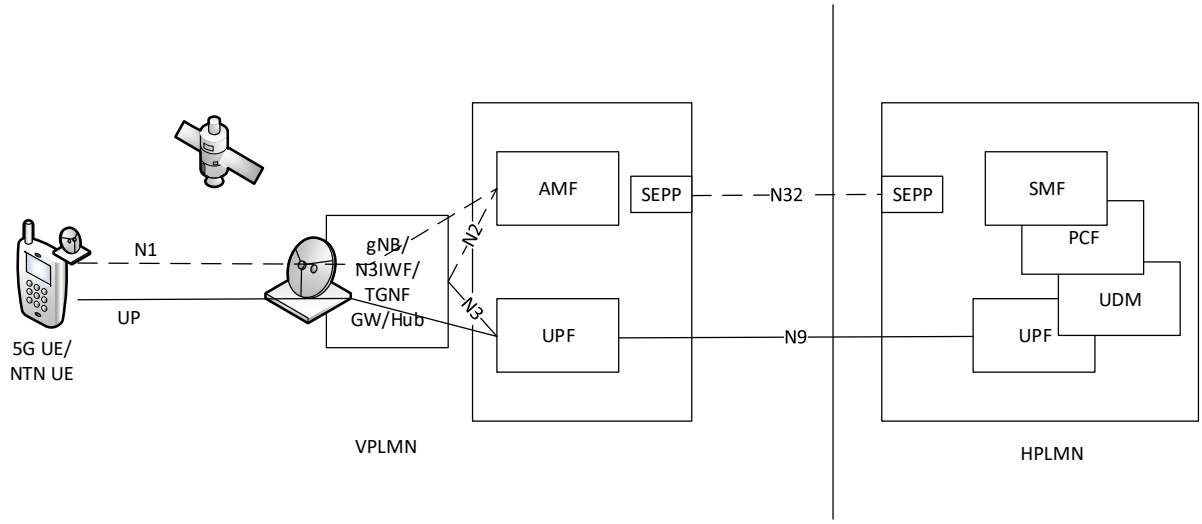

Figure 4-4: Satellite network as roaming partner of terrestrial networks

In this scenario the VPLMN (visited PLMN) is a satellite network with direct satellite access. In this network a 5G UE is having satellite access capabilities (i.e. acting as NTN UE). On the ground station side of the satellite network the satellite gateway (GW)/hub is acting as a 5G gNB in the case where the satellite network is supporting NR. In the case where the satellite network acts as non-3GPP access network, the GW/Hub will represent an N3IWF or a TNGF in case of untrusted and trusted non-3GPP access, respectively (see also Section 2.3.2 and Section 2.3.3).

Security threats and requirements

The security threats and requirements of this scenario are the same as those for the corresponding scenario with terrestrial access networks.

Existing security mechanisms

The existing security mechanisms apply that are used for the corresponding scenarios with terrestrial access networks (see Section 2.3.1, Section 2.3.2, and Section 2.3.3).

4.5 Security aspects of satellite access network integrated in terrestrial networks

The scenario for satellite network integrated with terrestrial network is depicted in Figure 4-5.

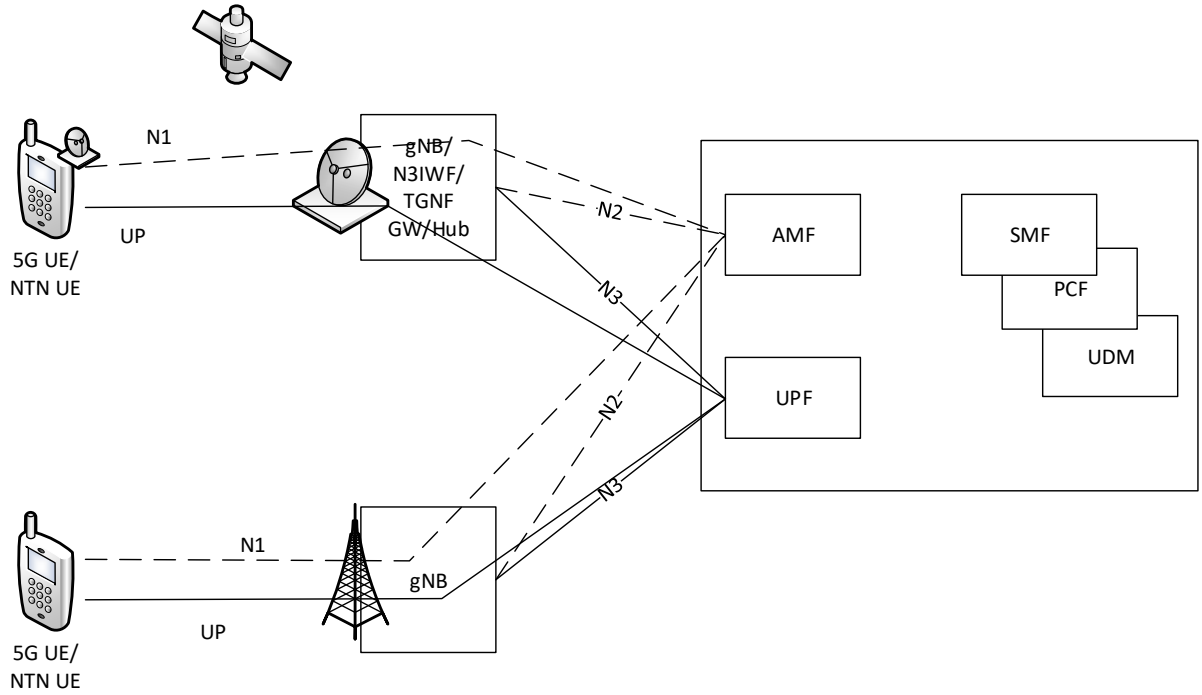

Figure 4-5: Satellite network integrated with terrestrial network

In this scenario the single mobile/satellite network consists of a single 5G core network with multiple types of access network. One of the access networks is based on satellite connectivity, other access networks are based on the traditional terrestrial access networks. For the satellite access network, the UE shall act as a 5G UE with satellite capabilities (i.e. an NTN UE). On the ground station side of the satellite network the satellite gateway (GW)/hub is acting as a 5G gNB in the case where the satellite network is supporting NR. In the case where the satellite network acts as non-3GPP access network, the GW/Hub will represent an N3IWF or a TNGF in the cases of untrusted and trusted non-3GPP access, respectively (see also Section 2.3.2 and Section 2.3.3).

Security threats and requirements

The security threats and requirements of this scenario are the same as those for the corresponding scenario with terrestrial access networks.

In a case where the satellite access network is share by multiple (terrestrial) core networks, there is an additional threat related to the sharing of satellite networks, i.e. access to other networks traffic and inappropriate usage of resources.

Existing security mechanisms

The existing security mechanisms apply that are used for the corresponding scenarios with terrestrial access networks (see Section 2.3.1, Section 2.3.2, and Section 2.3.3).

In addition, the sharing of the satellite access network needs to be provided in a secure way. For this there are no standardized mechanism as radio access network (RAN) sharing is provided as implementation options by vendors.

4.6 Security aspects of content delivery via satellite

In the case of content delivery via satellite the following aspects are assumed:

- Content is provided via some form of broadcast/multicast to multiple locations.
- Content may be stored in local caches near to the content consumers.
- Network elements such as MEC server and local core network functionality may be needed near to the local radio access elements.

Another aspect affecting the security of content delivery can be the mechanism used to retrieve content. A modern way of retrieving content is via MPEG DASH [13], which basically provides contents in smaller

pieces guided by an initial manifest file. This is different from the older technique where the content is provided as a single stream, or a single file containing the content.

Security threats and requirements

Security threats related to content delivery networks (CDN) are:

- DDOS attack on the CDN, e.g. due to active attacks or simply due to misconfigured clients;
- Content leakage, i.e. unauthorized access to content; this threat is aggravated by the local storage of content in content caches and the use of MEC servers
- Deep linking, i.e. access to a manifest file gives you access to all media segments; this is related to the use of techniques such as MPEG DASH.

Existing security mechanisms

Security mechanisms for protecting against the threats described above could be:

- Use token-based authentication;
- Use DRM (encryption of the content only reversible by a key) in combination with the use of TLS encryption to prevent man-in-the-middle attacks;
- Use token-based authentication for each request;

The above mentioned security mechanisms are not in scope of 3GPP standardization although they are partly based on other standards (e.g. IETF).

5 Complications with existing security solutions

5.1 Impact of usage of IPsec on satellite connections

As has been discussed in Section 2.4.1 it is common to have IPsec connections for backhaul. In the case of (untrusted or trusted) non-3GPP access IPsec is even mandated. For satellite connections this not beneficial for the following reasons:

- Satellite connections often make use of TCP acceleration techniques such as Performance Enhancing Proxies (PEP) (see, e.g. Section 7 of SaT5G D4.3 [14], and IETF RFC 3135 [15]). This is made difficult – if not impossible – where IPsec is used end-to-end, because PEP acts on the handling of TCP acknowledgements and IPsec encapsulates (and encrypts) the TCP connections (and makes it UDP).
- Satellite connections may make use of QoS differentiation, i.e. some connections will have different QoS than others. If all connections are mapped to the same IPsec connection before the connection reaches the satellite network, then the satellite network will only see a single connection and hence QoS differentiation is no longer useful.
- Satellite networks can often provide a form of multicasting, i.e. data transmitted from the ground station to the satellite is duplicated and sent to all (or a subset of) terminals. When using IPsec end-to-end over the satellite network this form of multicasting is no longer working, since IPsec only provides point-to-point tunnels.

In order to create awareness in 3GPP SA3, the above-mentioned complications have been discussed in a contribution to that group (see [16]). The reaction of 3GPP SA3, however, was that the options needed for enabling PEP etc. are available already (due to optionality of using IPsec, the optional interruption of encryption based on bilateral agreements, and the potential for using TLS), so the group did not see the need for any standardization.

5.2 Impact of satellite connections on security solutions and vice versa

A satellite connection may have a negative impact on 5G security solutions due to the added delay. Conversely 5G security solutions may have negative impact on satellite connections due to the added load. In order to assess whether or not these negative impacts exist, an investigation is made on the message exchange needed for each of the 5G security solution components (e.g. authentication, NAS signalling protection, radio interface (AS – Access Stratum) protection, privacy protection, security context handling during handover/mobility).

For 5G authentication the relevant message exchange is as depicted in Figure 5-1. The diagram also includes a number of timer values.

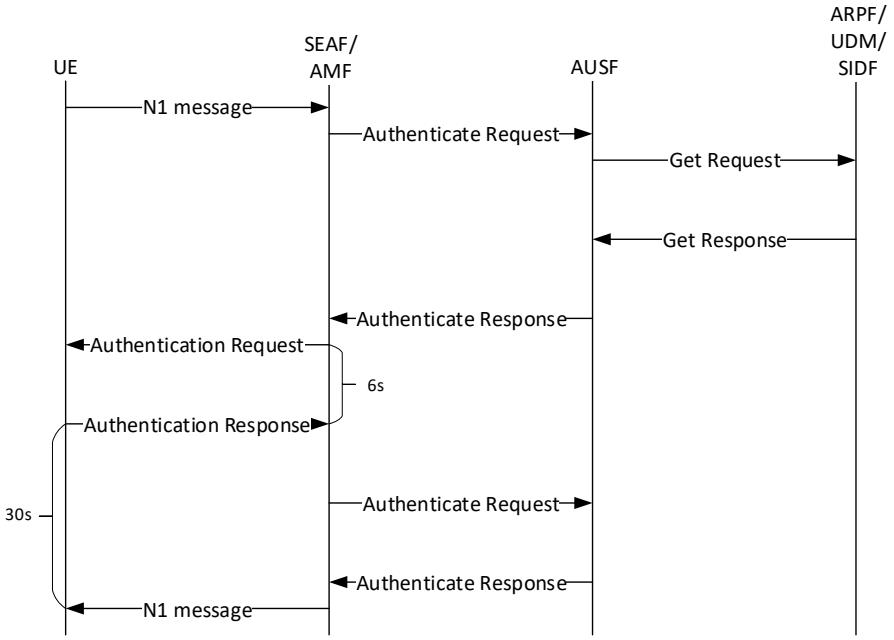

Figure 5-1: 5G authentication message flow with timer values

For establishment of the NAS security context the relevant message exchange is as depicted in Figure 5-2.

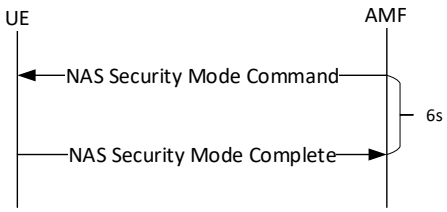

Figure 5-2: Establishment of NAS security context

For establishment of the AS security context the relevant message exchange is as depicted in Figure 5-3.

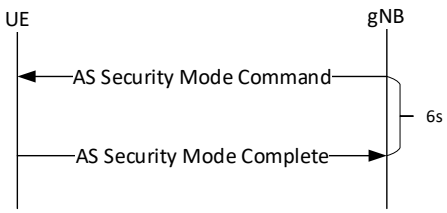

Figure 5-3: Establishment of AS security context

For handling of security context changes during handover/mobility the relevant message exchange is part of the standard RRC signalling. No new messages need to be exchanged between UE and gNBs.

The impact of delay caused by satellite connections, which may be as large as 300ms (one way) for geostationary satellites, is not expected to be significant in view of the typical timer of 6s for message sent from the network to the UE. Only in case of repeated re-transmissions of messages due to failures these network timers may become important. In Annex A the results of running a simulation investigating high latency, but especially high packet loss is shown. As can be seen, only in the case of extreme packet loss any significant impact on security procedure can be observed. And only in that case (with extreme number of re-transmissions) any impact of the higher latency may be observed. To

put this in context, due to the physical layer processing and technologies such as forward error correction together with adaptive coding and modulation, most satellite links operate as quasi-error-free links.

Within 3GPP SA2 as a result of a thorough analysis of UE and network timers (in TR 23.737 [17]), it has been concluded that for GEO satellites some of the UE timers may need to be adapted. It is proposed to adapt the registration procedure in order to enable the AMF to indicate to the UE that extended NAS timers are to be used.

As can be seen also in the above diagrams is the fact that security specific message exchanges are very limited in number of messages. It is therefore not expected that satellite connections will receive much load due to security solutions. Another observation that can be made is that exchange of keys over interfaces in general is minimized as such exchanges are usually considered security risks. Exchanges of keys is therefore kept to a minimum. A good example of this principle is the handling of security contexts during handover/mobility: instead of exchanging keys, only key identifiers and indications for key (re)generations are exchanged, in combination with local key generation (i.e. in the UE and in the network).

5.3 Integration of 5G security solutions with satellite networks

If a satellite network is used as transport network of a 5G network (e.g. for backhaul or interconnection – see Sections 4.1, 4.2, and 4.3), then there is little need for integration of 5G security solutions with satellite. It can be beneficial to have integration of management systems, but integration of network level functionality is not really required. The satellite network in this case can be proprietary, fully 5G, or use untrusted or trusted non-3GPP access technology.

If a satellite network is used as roaming partner of terrestrial 5G networks (see Section 4.4), then this puts requirements on the way authentication of UEs is performed:

- A UE that is 'subscriber' of the satellite network needs to fully support the 5G authentication requirements, i.e. it needs to have a USIM with key material matching the key material in the ARPF of the satellite network and the satellite network needs to fully support the 5G authentication procedures. Moreover, the satellite network and each roaming partner network need to have an interconnection where the roaming partner acts as VPLMN and the satellite network acts as HPLMN.
- A UE that is 'subscriber' of the terrestrial network and that needs to be able to roam in the satellite network is acting as a standard 5G UE and the terrestrial network and the satellite network need to have an interconnection where the satellite network acts as VPLMN and the terrestrial network acts as HPLMN. The satellite network in this case need to support the VPLMN functionality for support of 5G authentication.

If a satellite network is used as access network of a terrestrial 5G network (see Section 4.5), then this also puts requirements on the way authentication of UEs is performed:

- The UE will be a subscriber of the terrestrial 5G network and hence needs to conform fully to the 5G authentication requirements, i.e. having a USIM and supporting the 5G authentication procedures. Depending on the technique supported by the satellite network, the satellite access network will be considered a 3GPP access network, or an (untrusted, or trusted) non-3GPP access network. The satellite access network also needs to support the 5G security mechanisms for protecting the radio interface (i.e. the UE to gNB/ N3IWF/ TNGF interface), such as the support of the derivation of the appropriate keys.

If the satellite network is fully integrated in a relay architecture (see Section 4.3), it needs to comply to the security requirements (which are under development) for the relay architecture.

6 New security aspects

6.1 Slicing and virtual networking

When using satellite networks as transport network for multiple (terrestrial) networks, then it is useful to apply techniques such as network slicing or other virtual networking techniques in order to isolate the usage of the satellite network for each of its supported networks.

Within 3GPP network slice isolation is usually assumed without further need for additional specification. It is left to the implementation to ensure the validity of this assumption.

In virtual networks the various virtual resources (virtual machines and virtual networks) are usually well separated from each other. It is usually harder to get contact to virtual resources from outside a virtual machine, than it is to isolate it. Nevertheless, any requirement for isolation should be well managed by the virtual infrastructure management system.

6.2 Integrated MANO

Networks deploying both satellite networks and terrestrial networks in many cases need integration of their respective management systems (MANOs – Management and Orchestration).

Integration of management systems of different operators is not really considered within 3GPP (e.g. within 3GPP SA5). This seems to be an omission that would need to be addressed as it is vital for future integration of satellite and other networks.

The only indication of functionality that may help the needed integration is the 3GPP SA5 concept of Exposure Governance Management Function (see TS 28.533 [18]). Although not fully detailed this concept appears to resemble the Network Exposure Function (NEF) of 5G network. In [18] an example application of this Exposure Governance Management Function is depicted showing the way a management function MnF1 can be made available to a 3rd party via EGMF1 in a controlled way.

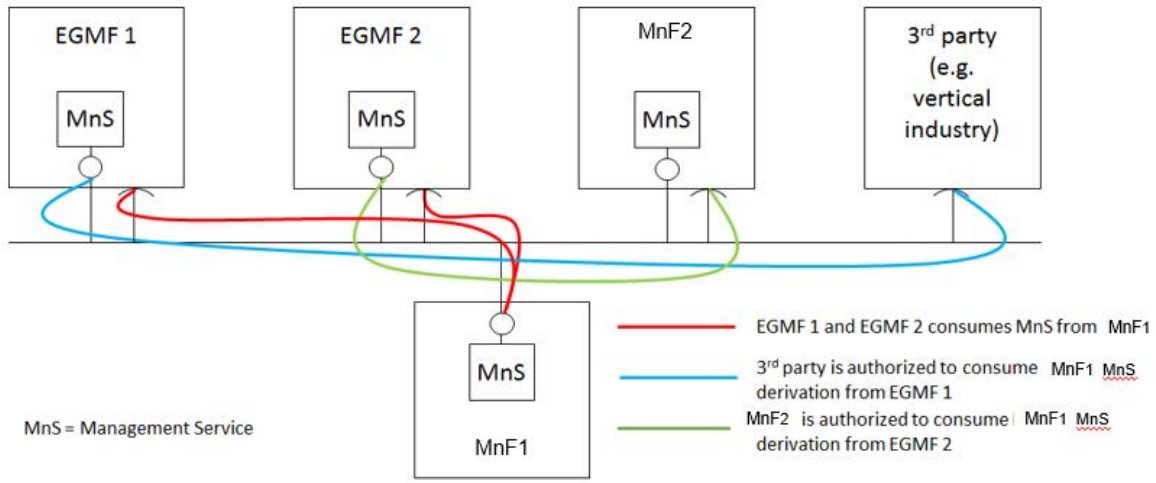

Figure 6-1: Example of the use of Exposure Governance Management Functions (TS 28.533)

6.3 Edge computing and caching/CDN

Edge computing, caching, and content delivery networking all are related to having functionality and content in a distributed (i.e. non central) location close to the consumers (of the content). Due to the fact that content is stored locally and is provided to consumers via local functionality additional security concerns may arise. However, from the point of view of 3GPP, this local storage and functionality is not considered to be in scope of 3GPP. Hence, no standardized security mechanisms shall be expected from 3GPP.

6.4 Multicast

As mentioned in Section 5.1, satellite networks often provide a form of multicast.

There are commonly two types of multicast. The first is that used for direct to home (DTH) TV broadcast. This does not usually use IP based multicast. These systems use a variety of different methods of data encryption usually closely linked to the operator's digital rights management. Traditionally the receiving set top box (STB) has a hardware card that acts like a SIM to determine which TV channels that STB is entitled to view and restricts the decoding to these channels. More modern STBs may use a software key based approach. All STBs do receive the same data stream at the physical and transport layers, the decryption is invoked at the time the content is viewed (either direct from the stream or saved on a local drive for later viewing).

Conversely many satellite broadband terminals (also commonly referred to as VSATs – very small aperture terminals) do support IP multicast (over UDP datagrams) and associated standards such as Internet Group Management Protocol (IGMP [19]). Different vendors approach the security of the IP multicast data differently. Some send the data in the clear (no encryption) and may use VLAN separation to restrict which sites can receive the data; whilst others generate a physical layer multicast encryption key that is managed by the VSAT NMS and only certain VSATs have the multicast decryption key and are able to decrypt the multicast data. Many IP applications that use IP multicast have their own application layer data protection schemes.

7 Conclusions and future work

7.1 Summary

Integration of satellite networks with 5G networks does not require many adaptations of standardized security solutions in 3GPP. In many cases, however, it does require the adoption of 3GPP security mechanism in satellite networks. It also requires the way satellite network and terrestrial networks cooperate with each other, and it may require a number of proprietary solutions. In this section a number of attention points for satellite networks are summarized.

1. Satellite networks need to adopt 5G authentication and other security procedures if they want to act as roaming partners or if they want to be tightly integrated into terrestrial networks.
2. Satellite networks need to provide (virtual) network isolation (e.g. slice isolation) if they want to be provided as transport network for multiple terrestrial networks.
3. Satellite networks need to cooperate with terrestrial networks in order to enable TCP acceleration and QoS differentiation over backhaul. This cooperation could result in a different way of providing security than is currently common practice in terrestrial networks (i.e. monolithic end-to-end IPsec), e.g. by providing PEP outside the IPsec tunnel (i.e. IPsec is not provided end-to-end), or by temporarily decrypting and re-encrypting around the PEP nodes. It might also result in the use of other encryption techniques such as TLS instead of end-to-end IPsec.
4. Satellite network and terrestrial network cooperation may benefit from secure integration of management systems. Integration of management systems can benefit from complying to 3GPP standards (e.g. from 3GPP SA5).
5. The standard timer values used in the 5G network in security procedures appear to work over satellite links other than in exceptional and unlikely circumstances. There is no need to change their values. With respect to timer values in the 5G devices, 3GPP has recognized a potential need to update those. Standardization work is ongoing for this issue.
6. There is no need to change key management in 5G networks in case satellite connections are used for access, backhaul, or interconnection.
7. Satellite networks may benefit – for the short to medium term – from the use of trusted non-3GPP access which has recently (2019) been standardized by 3GPP in the TNGF.
8. For securing content delivery, content caching, and edge computing, mostly proprietary solutions need to be developed.
9. Use of multicast in satellite networks may require security solutions going beyond the state of the art. It is not clear if 3GPP standardized solutions will become available that fully fit the way multicast is used in satellite networks.

7.2 Recommendations for future work

The SaT5G project can make the following recommendations:

1. Satellite equipment vendors and operators need to develop their solutions to 5G authentication and other security procedures to allow tighter integration.
2. The adoption and implementation of TNGF should be further studied and tested in the satcom context allowing the satellite element to be trusted.
3. The extension of security and trust in to MANO and business planes could usefully be further investigated.
4. Satellite networks should look to maintain and increase focus in the support of 3GPP access if they want to provide direct satellite access.
5. Investigation should be done of possible interactions between 5G security mechanisms, DRM and satellite enabled multicast content distribution.

8 References

[1] 3GPP TS 33.501, “Security architecture and procedures for 5G system”.

[2] 3GPP TS 23.501, “System Architecture for the 5G System (5GS); Stage 2”.

[3] D3.1, “Integrated SaT5G General Network Architecture,” SaT5G, WP3.1, 2019.

[4] 3GPP TR 38.874, “Study on Integrated Access and Backhaul”.

[5] 3GPP TS 38.300, “NR and NG-RAN Overall Description;”.

[6] 3GPP TR 33.824, “Study on Security for NR Integrated Access and Backhaul”.

[7] 3GPP TR 33.855, “Study on security aspects of the 5G Service Based Architecture (SBA)”.

[8] Gilat, “SkyEdge-II-c-Capricorn-PLUS data sheet,” [Online]. Available: https://www.gilat.com/wp-content/uploads/2019/04/Gilat-Product-Sheet-SkyEdge-II-c-Capricorn-PLUS.pdf. [Accessed 11 2019].

[9] Newtec, “SECURING VSAT TERMINALS,” 28 04 2014. [Online]. Available: https://www.newtec.eu/article/article/securing-vsat-terminals. [Accessed 11 2019].

[10] ETSI EN 302 307-1, “Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2,” 2014.

[11] ETSI EN 302 307-2, “Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, New Gathering and other broadband satellite applications, Part 2: DVB-S2 Extensions (DVB-S2X),” 2015.

[12] Hughes Network Systems, “JUPITER™ System with DVB-S2X,” [Online]. Available: https://www.hughes.com/sites/hughes.com/files/2018-07/JUPITER-System-DVB-S2X_H52630_071218.pdf. [Accessed 11 2019].

[13] ISO/IEC 23009-1, “Dynamic adaptive streaming over HTPP (DASH); Part 1: Media presentation description and segment formats,” 2014-05-15.

[14] D4.3, “Multi-link and Heterogeneous Transport - Analysis, Design and Proof of Concepts,” SaT5G, WP4.3, 2019.

[15] IETF RFC 3135, “Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations,” 2001.

[16] 3GPP S3-192527, August 2019. [Online]. Available: https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_96_Wroclaw/Docs/S3-192517.zip.

[17] 3GPP TR 23.737, “Study on architecture aspects for using satellite access in 5G”.

[18] 3GPP TS 28.533, “Management and orchestration; Architecture framework”.

[19] IETF RFC 3376, “Internet Group Management Protocol, Version 3,” 2002.

[20] 3GPP TS 24.501, “Non-Access Stratum (NAS) protocol for 5G System (5GS); Stage 3”.

Annex A: the effect of packet loss on security procedures

At the start of this project it was unclear whether the inclusion of a satellite backhaul connections would be on security procedures. One of the assumptions was that procedures would fail due to high packet loss and high latency. One of the activities that was set out to be performed in SaT5G was therefore to estimate a high packet loss and high satellite link and to test out whether a UE would be able to complete a so-called IMSI-attach. In the following sections, we explain our simulation environment and test setup and present our results. Note that the simulation is sometimes using 4G message terminology, since it was created before the final naming of all the 5G messages was completed. The results, however, also apply to 5G networks as the procedures for authentication are very similar.

A.1 Simulation environment

In our simulation environment, we assumed a single UE that would boot up. In order to get a data connection, the UE would have to first attach, then authenticate and setup the security. Only once that is done can the UE request data bearers and start sending data. For our simulation environment, we simulated both the UE and AMF state machine including timers and time outs according to 3GPP TS 24.501 [20]. The state machine that we simulated can be visualized as depicted in Figure A-1.

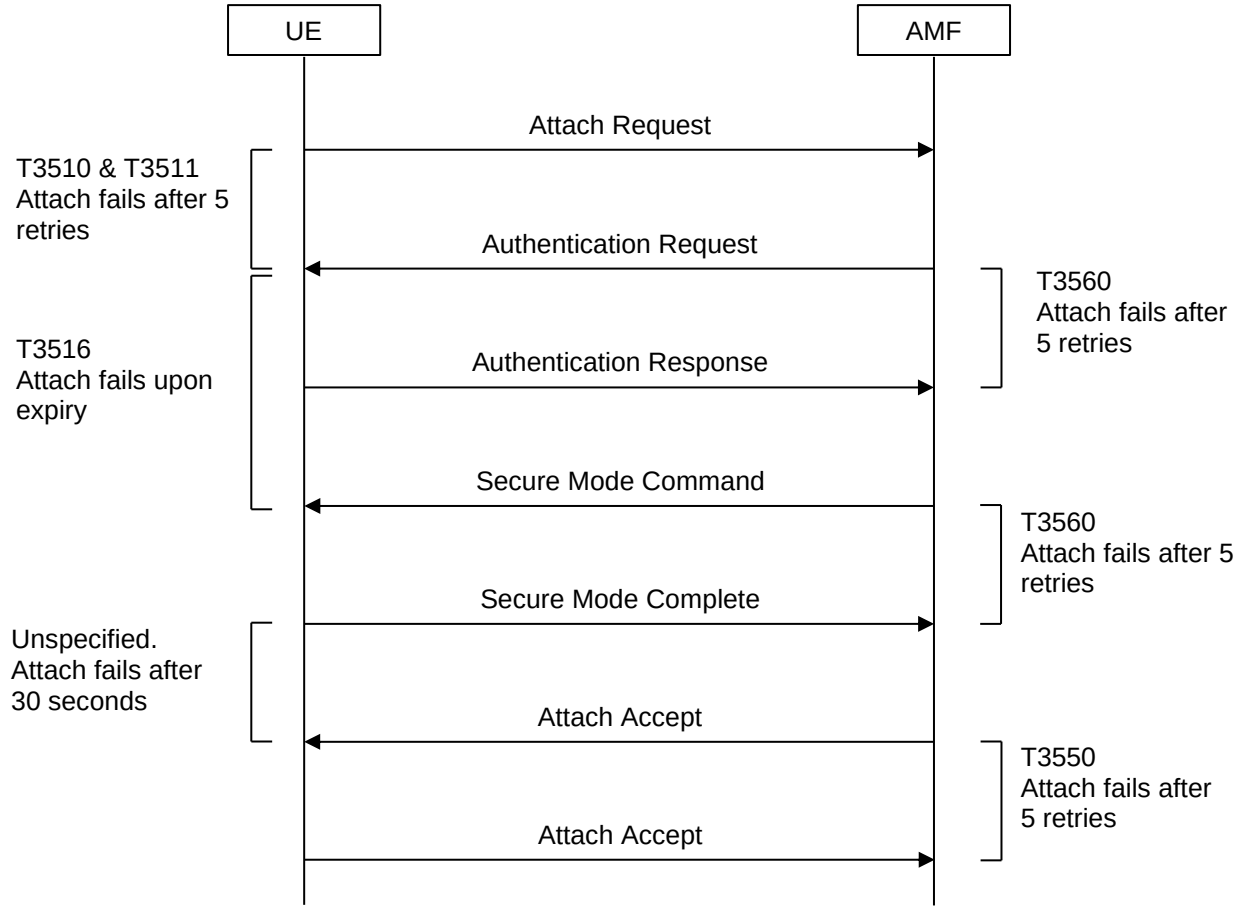

Figure A-1: An overview of the model used in our simulation for initial attach by a UE.

The behaviour is as follows:

- The UE sends an attach message. It sets timer T3510 which lasts 15 seconds. Upon expiry (i.e. if the UE hasn't received a message from the AMF), the UE sets timer T3511 and once that timer expires it sends a new attach request. When the timers time out after the UE has sent the fifth attach request, the UE should set T3502 which lasts 12 minutes by default. In our simulation we don't set T3502, but let the attach procedure fail.
- Upon reception of the attach request, the AMF sends the authentication request. In our simulation, we assume that the AMF can get the authentication vectors instantly. In a real-life situation, this will take some time. When the AMF has sent the message it sets T3560 which

lasts 6 seconds and upon expiry it will retry. After the AMF sends 5 authentication requests upon which it doesn't get a response, the AMF will assume that the UE is no longer present in its network and forgets the UE. Our simulation then counts this authentication run as failed.

- When the UE receives the authentication request, it will send the authentication response and start the timer T3516. If the authentication response fails to be transmitted, the UE will receive a new authentication request with the same parameters from the AMF after the time-out of timer T3560. That is, there is no mechanism on the UE to trigger retransmission on its own. It will always just respond to a message from the AMF. Due to this effect, the maximum tolerable number of message of the authentication request and response together is 5.
- After reception of a correct authentication response, the AMF will send the secure mode command and start timer T3560 (again). After 5 retries, it will assume that the UE cannot receive the secure mode command and fail the authentication run. In this case, our simulation assumes that the authentication run has failed.
- When the UE has received the secure mode command, it will reply with a secure mode complete and set a timer of 30 seconds after which it will consider the authentication failed if it does not receive a attach accept message from the AMF.
- Once the AMF receives a correct Secure Mode Complete message, the AMF will send the attach accept message and start timer T3550. Also for this message, the AMF will fail the authentication procedure if it has to send the message more than 5 times without receiving a Attach Accept from the UE as well.
- Finally, the UE receives the Attach Accept and responds with the Attach Accept message back to the UE.

As can be observed from the behaviour description, the timers and retries are initiated by the AMF. This means that packet loss on the downlink between the AMF and the UE and packet loss on the uplink between the AMF and UE both affect the completion ratio of the authentication procedure. In case of a high packet loss, this would lead to retransmissions, which are generally not favoured by security people and high latency would lead to timers timing out which would lead to a reset state machine.

A.2 Running the simulation

The above model describes how the interactions between one single UE and one AMF are. In our simulation, we have run the simulation for different scenarios and for 10 000 attach procedures in order to understand the effects.

The characteristic variables of the satellite communication are the latency and the packet loss. The latency can affect the success rate in case the latency causes timers to time out and therefore causes failure. The packet loss causes the success rate because of the possibility that not all necessary messages will get through. In principle, the simulation should therefore have been a parameter space investigation where we would vary both latency and packet loss.

After careful consideration, we decided to not run separate runs for latency. The reason is that in order for latency to affect the success rate, the latency has to be of the order of the value of the timers, e.g. roughly 6 seconds. A GEO satellite one-way latency is usually not higher than 300 ms. Hence, even when assuming an extreme satellite networks latency of 0.5 s or less, there is little realistic value in increasing the latency. Also, once the latency is increased to be of the order of the timers, the procedure would always fail, which can only be solved by increasing the value of the timers. The shortest timers all live on the AMF, such that an operator could configure that individually for requests coming via a particular link.

So, the scenarios that we investigated were scenarios with increasing packet loss from 0 % to 50 % with increments of 10 %. It should be noted that such high rate of packet loss are not typical for satellite links. It does show, however, the theoretical effect of such packet loss rate.

A.3 Results of the simulation

The effects of satellite backhaul on security procedures have been simulated using an implementation of the state machine according to TS 23.501 [2]. The following has been observed:

- The relation between the satellite transmission error and the attach completion procedures is non-linear. For a transmission rate of 80 % (i.e. 20 % of the packets gets lost) 2.5 % of the attach procedures is not completed. A 50 % packet loss leads to an attach completion rate below 40 %. This is shown in the left pane of Figure A-2.

- The average time that it takes to complete the procedure increases linearly with the packet error rate. The spread between minimum completion time and maximum completion time, however, increases rapidly with increasing packet loss. This is shown in detail in the right pane of Figure A-2.The figures below describe this in more detail:

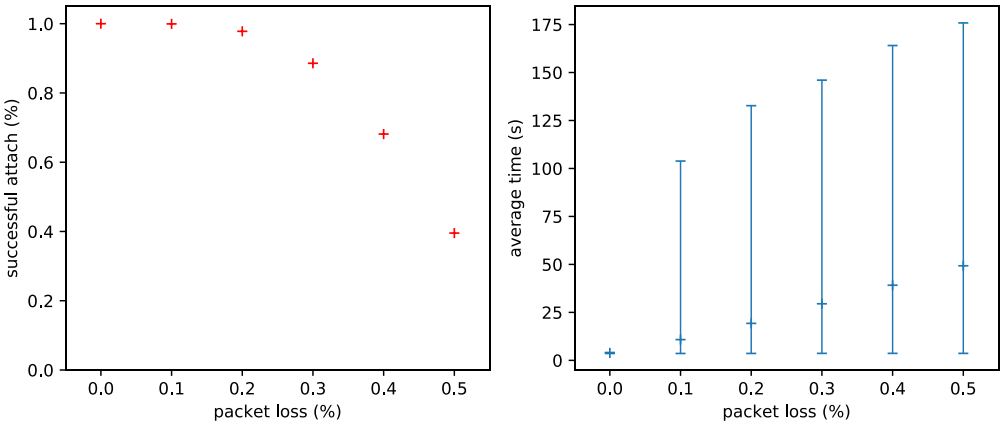

Figure A-2: Two panes showing the results of the simulation of 10 000 UEs running an authentication procedure. The left pane shows the success rate of the attach procedure. The right pane shows the average time (the middle cross) and the maximum and minimum time of the completion of the procedure.

For completeness sake, we included the numbers on which Figure A-2 is based in the table below as well:

Table A-1: Results of simulation

Packet loss	Average time (s)	Minimum time (s)	Maximum time (s)	UEs attached (#)
0 %	3.8	3.6	4.1	10000
10 %	10.8	3.6	103.9	9994
20 %	19.3	3.6	132.7	9780
30 %	29.5	3.6	146.0	8857
40 %	39.2	3.6	164.1	6814
50 %	49.3	3.6	175.8	3954