|  |
| --- |
| **5G ONE4HDD SECURITY STRATEGY**  22nd December 2023  Authors: Haitham Cruickshank |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Details of document preparation and issue:** | | | | | | |
| **Version no.** | **Prepared** | **Checked** | **Reviewed** | **Approved** | **Issue date** | **Issue status** |
| 1.0 | H. Cruickshank |  | Alex Buchan |  | 12 Dec 2023 | Draft |
| Final | H. cruickshank |  | Alex Buchan, David Owens |  | 21 Dec 2023 | Final |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Executive Summary

This deliverable presents the security strategy guidance for the 5G ONE4HDD with top level threat analysis, requirements and recommendations, which will be elaborated at the next security task.

The 5G ONE4HDD, proposes a novel solution to optimise mobile network performance in High Demand Density (HDD) environments such as music festivals, sporting events, and major public gatherings. The aim is to design and deploy a Mobile 'Cell on Wheels' equipped with Open RAN (ORAN) technology or the equivalent tier 2 RAN equipment.

At the heart of this project, there several multicast broadcast technologies such as the 4G enhanced Multimedia Broadcast/Multicast Service (eMBMS) and the 5G Multimedia Broadcast Multicast Service (MBS). It supports content distribution to a wider audience via; a broadcast and/or multicast distribution model, providing high spectral efficiency.

Section 1 starts with an introduction unicast, multicast and broadcast concepts. It highlights the differences between multicasting and broadcasting. As such, the large-scale distribution of real time streaming IP packets can be broken down into two steps:

* First step is the wide area distribution using multicasting.
* Second step is delivery to customers in the RANs using broadcasting (or multicast if possible).

Therefore, multicast security provides a flexible way to manage security and key management for such services. Section 1 presents an overview of unicast and multicast security with a comparison between a flat key and binary tree distribution (see Figures 2.0 and 3.0) and key management scalability issues for large groups are discussed (examples here are the multicast users in HDD environment).

Section 2 presents an overview of the eMBMS and the MBS multicast/broadcast architectures. This helps to create some context for the security analysis in sections 3, 4 and 5. The 5G ONE4HDD service platform consists of four main components: cameras, Multi-access Edge Computing (MEC), a broadcast/multicast core network, and RAN/ORAN and this makes the basis for the security analysis in the following sections.

Section 3 presents the European Union Agency for Network and Information Security (ENISA) guidelines on the threat assessment for 5G mobile network and using the related 3GPP specifications [1] and the threat map in Annex B1 [13] and the security assurance methodology in Appendix B2 [14].

There is a wide range of threats that affect 5G networks, however and in relation to 5G ONE4HDD architecture and components, the following threats have highest likelihood and highest impact:

* Generic threats: These are threats that typically affect any ICT system or network such as Denial of Service (DoS) threat.
* Core and Open RAN (ORAN) threats: The majority fall under the categories of ‘Nefarious activity/abuse’ and ‘Eavesdropping/ Interception/ Hijacking’.
* Multi-edge computing (MEC) threats: These threats relate to components located at the edge of the network. The majority fall under the categories of ‘Nefarious activity/abuse’ and ‘Eavesdropping/ Interception/ Hijacking’.
* eMBMS/MBS multicasting threats: such as Unauthorised access to eMBMS/MBS entities and the user data and services.

Section 4 builds on top of the threat information provided in section 3 and presents the security requirements for the major components in 5G ONE4HDD architecture such as 4G/5G ORAN and Core; MEC and eMBMS/MBS. Examples of such requirements are: user data and signalling data confidentiality and integrity; also the authentication and authorisation for the gNB (ORAN) setup and configuration plus others. All the these requirements could be satisfied by following the ORAN Alliance and 3GPP security specifications TS 33.501 [10].

Section 5 presents the security recommendations for the major components in 5G ONE4HDD:

1. Between the MEC and eMBMS (or MBSTF in MBS): The Transport Layer Security (TLS)/Datagram TLS (DTLS) are recommended. This will provide access control (authentications and authorisation) plus confidentiality and integrity protection. This approach is compliant with the ORAN Alliance recommendations. Optional security is also possible for other unicast hops in the network such as using TLS between content provider (e.g. cameras) and the MEC.
2. In relation to the secure broadcasting/multicasting that was discussed in Section 1, DTLS is recommended as the end-to-end security solution between the Content provider and a group of UEs.
3. The mobile network core and ORAN: Implementing the 3GPP security specifications such as TS 33.501 [10], should be adequate to satisfy the security requirements in section 4.1. This includes the UE and network authentication and authorisation, plus data and signalling confidentiality and integrity protection.
4. Regarding key management, the use of the flat-key system (see Section 1) is recommended for static groups (fixed membership) and LKH is recommended for large dynamic groups (changing membership). It is agnostic to the 4G/5G technologies. It can also bridge the security gap between mobile and broadcast operators.

Section 6 presents the next steps for the security work. At this early stage of the ONE4HDD project, Figure 12.0 shows a simplified security architecture for ONE4HDD. More elaborate security architecture will be defined at the later stages of the project. The security strategy first step is focused on the unicast security between the MEC and Scheduler and Broadcast Controller (RAN tier 2) using techniques such as Transport Layer Security (TLS). Also and in relation to the HDD challenging environment, the second step is the Multicast security design Proof of concept using simulation demo for securing 5G ONE4HDD end-to-end user traffic.

The security research will focus on secure multicasting and broadcasting. Looking ahead towards 6G, secure multicasting/broadcasting will need to be dynamic and scalable for large groups that could be distributed in wide areas. This also might include 3D networks (including satellites, drones and High-Altitude Platforms, HAPS). The ONE4HDD research is focused on using Logical Key Hierarchy (LKH), as described in section 1. This research will also cater for future use cases where multicast groups could span large geographic areas (e.g. multicast users are spread through several major cities, like a popular football game) and multiple administrative domains (e.g. multiple mobile operators and cloud providers).

Finally, this document has been developed to follow the principles outlined by DSIT in their recommendations for the ONE Programme - Security Strategy (in the FGA). This includes a list of topics to be addressed: such as more detailed threat and risk analysis, as the project architecture progresses, plus the mitigation and implementation plans.

Broadly speaking, all the relevant topics in the list of priority security research and development areas in the FGA are covered in this deliverable.

**5G ONE4HDD Security Strategy**

[Executive Summary 2](#_Toc154050381)

[1. Introduction 6](#_Toc154050382)

[1.1 Multicast and broadcast overview 6](#_Toc154050383)

[1.2 Unicast/Multicast security overview 8](#_Toc154050384)

[2. ONE4HDD multicasting/broadcasting approach 10](#_Toc154050385)

[2.1 enhanced Multimedia Broadcast Multicast Service (eMBMS) architecture 10](#_Toc154050386)

[2.2 5G Multicast Broadcast Services (MBS) architecture 12](#_Toc154050387)

[3. Threat Analysis 14](#_Toc154050388)

[3.1 5G Generic Threats 16](#_Toc154050389)

[3.2 Open Radio Access Network (ORAN) Threats 17](#_Toc154050390)

[3.3 Multi-access Edge Computing (MEC) Threats 18](#_Toc154050391)

[3.4 Multicasting using eMBMS/MBS threats 19](#_Toc154050392)

[4. Security Requirement 20](#_Toc154050393)

[4.1 Security Requirements for 4G/5G ORAN and Core 20](#_Toc154050394)

[4.2 Security Requirements for MEC 21](#_Toc154050395)

[4.3 Security Requirements for eMBMS/MBS 22](#_Toc154050396)

[5. Security Recommendations 22](#_Toc154050397)

[6. Next Steps 23](#_Toc154050398)

[6.1 Simplified ONE4HDD security architecture 23](#_Toc154050399)

[6.2 security research and development areas 24](#_Toc154050400)

[Annex A - Acronyms 26](#_Toc154050401)

[Appendix B: 5G Threat Map and security assurance 28](#_Toc154050402)

[B.1 5G Threat Map 28](#_Toc154050403)

[B.2 The 3GPP Security assurance Methodology (SECAM) 28](#_Toc154050404)

[Appendix C: ONE4HDD IP ARRANGEMENT 30](#_Toc154050405)

[REFERENCES 31](#_Toc154050406)

5G ONE4HDD Security Strategy

# Introduction

## Multicast and broadcast overview

At the heart of this project, there several multicast broadcast technologies such as the 4G enhanced Multimedia Broadcast/Multicast Service (eMBMS) and the 5G Multimedia Broadcast Multicast Service (MBS). It supports content distribution to a wider audience via; a broadcast and/or multicast distribution model, providing high spectral efficiency.

The previous project (5G VISTA) service platform mainly consisted of four main components; cameras, Mobile Edge Computers (MEC), a broadcast/multicast core network, and 5GNR NSA RAN as described in Figure 1.0 below. The ONE4HDD will follow a similar approach, but some of the components will be different such as using alternatives to the R&S BSCC (eMBMS related) will be explored.

A diagram of a computer network

Description automatically generated

Figure 1.0 - an overview of the system architecture for “Going glass to glass”.

The 5G ONE4HDD, proposes a novel solution to optimise mobile network performance in High Demand Density (HDD) environments such as music festivals, sporting events, and major public gatherings. The aim is to design and deploy a Mobile 'Cell on Wheels' equipped with Open RAN (ORAN) technology, offering reliable connectivity in crowded venues. The technical approach involves the development of a portable cell site, capable of serving hundreds of users simultaneously. This cell site will utilise cutting-edge ORAN technology (or equivalent technologies) and advanced codecs to ensure high-quality data transmission even in the busiest environments. The project also explores the provision of services such as Over The Top (OTT) video, social media, emergency broadcasts, and standard telephony. To achieve these objectives, multicasting and broadcasting will be used, which produces unique challenges in terms of security. As such one of the project objectives is provisioning of Network Security, Reliability and Resilience, ensuring that ORAN and multicasting solutions are secure and resilient against cyber threats while maintaining high reliability. The project approach to security will be compatible with the ORAN Alliance and 3GPP recommendations.

Let us start with a brief comparison between unicast, broadcast and multicast [2]:

* Unicast: enables traffic, such as file transfer and real-time streaming of IP packets, to move across networks from a single transmitting point to another single receiving point. One-to-one bidirectional communications is the foundation of the Internet and cellular networks, from GSM right up to the current LTE/4G and 5G technologies.
* Broadcast: traffic flows from a single point to all possible endpoints that can be reached within the network. This is the easiest and most efficient way to ensure traffic reaches its destination, but has very high networking overheads. This distribution mode has been used for many years on the Internet (but sparingly with a limited number of hops to reduce replication – broadcast storms - and traffic volume). Also broadcasting is used for free-to-air analogue TV and radio distribution. Today it is mainly used in digital television and video/audio distribution networks. The most common technology is called Digital Video Broadcasting (DVB).
* Multicast: enables traffic to exist between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast is a “one source to many destinations” approach to traffic distribution. In other words, it only involves the destinations that choose to accept the data from a specific source and receive the traffic stream. Multicasting is well understood in the Internet community and there has been (in past) some effort to develop IP multicast-user management (such as the Internet Group Management Protocol, IGMP, [IETF RFC 3367]) and IP multicast-routing protocols (such as the Protocol Independent Multicast-Sparse Mode, PIM-SM, [IETF RFC 7761]).

Before addressing the security issues more deeply, let us set the scene with a challenging research example from recent sporting events to give context to broadcasting and multicast on a large scale and set the scene for an expanded research vision 5G ONE4HDD solution into the future: In July 2021, the Euros football final game between England and Italy was in London and watched by about 30 million people (roughly) in UK and let assume that another 30 million watched it in Italy, plus 70 million in the rest of Europe and the world (total of 130 million users). This was delivered using mostly the DVB (with its variations such as DVB-T, DVB-C or DVB-S for terrestrial, cable and satellite channels). Therefore, the challenge is how such large distribution can be achieved in 4G/5G networks, which is not compatible with DVB standards. This question will be answered (at least from security perspective) later in the document.

There have been attempts in the past to adopt DVB into the 3GPP mobile network but that has failed because:

* This solution requires specialized base stations, which are separate from the cellular infrastructure.
* The spectrum utilized by this solution is distinctly separate from that used to provide cellular services; which makes it very expensive.
* The User Equipment (UE) needs to have additional hardware installed in order to support reception of DVB broadcasting;

Therefore, a future eMBMS/MBS solution must consider other alternatives (instead of DVB) to deliver such a sporting event to 130 million people spread across several countries, several Mobile Network Operators (MNO) and several Radio Access Network (RANs) within each MNO domain. Providing security will add another layer of complexity to this challenging communications problem.

The lessons learnt from the Internet dictates that broadcasting should be confined to the RANs, where the interested subscribers are located. The IP multicast concept could be used for the wide area distribution of live streams (e.g. from cameras in the stadium) to all the MNOs and RANs/ORANs across the world that have subscribers. IP multicast (with its related IGMP and PIM-SM protocols) could be used for such distribution as stated in the eMBMS specifications 3GPP TS 23.246 [4] and TS 26.346 [5]. However, other and more efficient private multicast routing within each MNO domain could also be used, deploying the Software Defined Networking (SDN) technology.

In summary, the distribution of real time streaming IP packets can be broken down into two steps: First step is wide area (across the world) distribution using multicasting; and the second step is the delivery to customers in the RANs using broadcasting or multicasting.

## Unicast/Multicast security overview

Many current unicast communications use the Internet Engineering Task Force (IETF) Transport Control Protocol (TCP) as a reliable end-to-end transport protocol that sits above IP layer in the protocol stack and the Transport Layer Security (TLS, [IETF RFC 5246]) is the protocol of choice to provide end-to-end security. However, for broadcasting and multicasting applications (such as live video streaming, which is 5G ONE4HDD data traffic), it is not possible to use TCP for delivery and hence the preferred protocol is the User Datagram Protocol (UDP), which does not provide reliability (ordered delivery without duplication or loss). UDP is also suitable for multicasting and broadcasting. However, TLS requires the use of TCP and it does not work with UDP and hence the security protocol of choice for UDP is Datagram Transport Layer Security (DTLS, IETF RFC 6347]).

From the security perspective, broadcast security is very challenging, and it is very difficult to go beyond simple content encryption with a key that is distributed to all users before the event. DVB security is weak and had suffered in the past from smart-card (that is used inside the TV setup-box) forgeries. Also key management for dynamically changing subscription membership is very difficult for large events (such as the 130 million users in the football example).

Multicast security provides a more flexible way to manage security more efficiently. There was a large volume of work within the Internet Engineering Task Force (IETF) on protocols for secure multicasting such the Multimedia Internet Keying (MIKEY, [IETF RFC3830]) and using the Logical Key Hierarchy (LKH, [IETF RFC 2627]) and its variations to tackle large scale key management.

Regarding key management issues such as key distribution and rekeying, comparison between a flat key and LKH is shown in Figure 2.0 below, where the flat key system is more suitable for static groups and LKH is more suitable for large and dynamically changing group membership (users joining and leaving the group all the time such as HDD environment). Rekeying is required to protect forward security (preventing past users from access to future data) and backward security (preventing a new user from having access to past data).

Figure 3.0 shows the potential scalability of LKH. In the case of 134 million users for example, for a flat key system, to do a rekey to exclude one multicast member, there will be a need to transmit 134 million – 1 keys (a new key to the remaining members).

However, if using LKH, 134 million = ~ 227 and the number of rekeys is 2log 227 – 1 = 53. Therefore only 53 short messages are required and all of them can be concatenated into a single message that is multicast to all members.

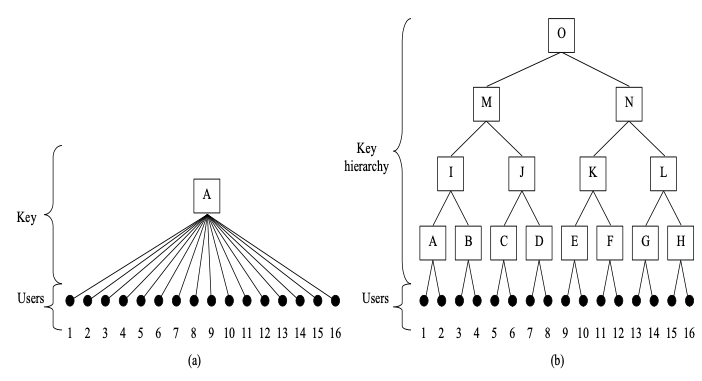


Figure 2.0 - Logical Key Hierarchy (LKH) key distribution: (a) Flat key (static groups), (b) binary tree (dynamic groups)

A graph with red text

Description automatically generated

Figure 3.0 - LKH scalability graph

More details on LKH and 5G ONE4HDD multicast security design will be provided in future deliverables.

The following sections examine the 5G ONE4HDD system components and the multicast architecture in more detail and then followed by threat analysis and security recommendations.

# ONE4HDD multicasting/broadcasting approach

To give some 5G network context to the 5G ONE4HDD system, let us introduce the three sets of 3GPP 5G Use Cases, as presented in the European Union Agency for Network and Information Security (ENISA) report [[ENISA report on 5G threats]:

* Enhanced mobile broadband (eMBB): Defined as an extension to existing 4G broadband services, eMBB will be the first commercial 5G service enabling faster and more reliable downloads and uploads.
* Ultra-reliable low latency communication (URLLC): Designed to support mission critical communication scenarios, such as emergency situations, autonomous systems operations, among others.
* Machine Type Communications (MTC): This can be further classified as ‘massive machine‐type communication’ (mMTC) and ‘ultra‐reliable machine‐type communication’ (uMTC).

The 5G ONE4HDD system with its core eMBMS/MBS technology, falls in the eMBB use case category. The multicast/broadcast technology at the heart of this project. It supports content distribution to a wider audience via a broadcast and/or multicast distribution model, providing high spectrum efficiency. In the deliverable will exam the eMBMS and MBS architecture and related security issues.

## enhanced Multimedia Broadcast Multicast Service (eMBMS) architecture

This section presents a high-level overview of the eMBMS architecture and protocols. This helps to give some context and background for the related security threat analysis in the following sections.

The Multimedia Broadcast/Multicast Service (MBMS) was devised to offer both broadcast and multicast service over the 3G/4G network. The Broadcast-Multicast Service Centre (BM-SC) processes MBMS specific activities (e.g., authorising UEs that request MBMS service, managing MBMS sessions, and interworking MBMS services of different network operators in roaming scenarios).

MBMS was enhanced to eMBMS. The architecture of eMBMS there are several entities in addition the BM-SC, as show in Figure 4.0 below. Namely, Multi-cell/multicast Coordination Entity (MCE) and MBMS Gateway (MBMS-GW). MCE serves one or more eNodeBs (eNBs), allocates radio resources used for MBMS transmissions, and is involved in the signalling of MBMS session control. MBMS-GW sends/broadcasts MBMS packets to the eNBs that are transmitting the broadcast / multicast service, and it controls the MBMS sessions in the evolved UTRAN (E-UTRAN) via Mobility Management Entity (MME). Therefore, unlike MBMS, more granular control of the Radio Access Network (RAN) entities is possible with these new eMBMS entities.

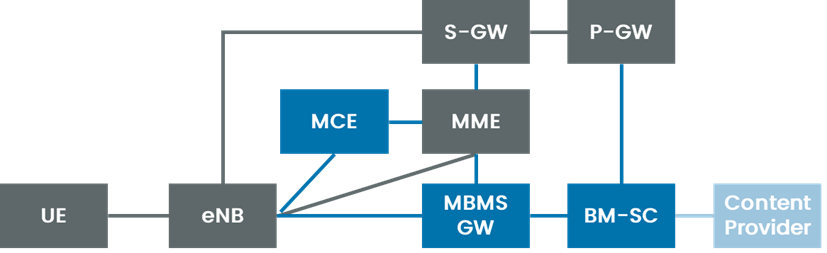


Figure 4.0 eMBMS architecture (3GPP TS 23.246 v14.2.0 and 3GPP TS 36.300 v14.9.0)

In addition, eMBMS introduced the concept of MBMS Single Frequency Network (MBSFN) to deliver the broadcast/multicast service. MBSFN is a transmission technique where identical waveforms are transmitted at the same time via a group of cells covering a geographic area. Alternatively, from Release 13, Single Cell Point to Multipoint (SC-PTM) can be used to adjust the broadcast/multicast area with the granularity of a single cell and to dynamically use radio resources of each cell.

Within the MBMS-GW it is possible to enable distribution of eMBMS payload by using IP Multicast in the backbone network. IP Multicast distribution is done from the MBMS-GW to eNodeB or RNC downstream nodes. The Source Specific Multicast (SSM) service model is recommended for use by nodes and routers as specified in [IETF RFC 4607] and [IETF RFC 4604].

The content provider and the BM-SC authenticate each other for performing service management and status reporting and notifications. During this authentication step, the content provider and the BM-SC exchange their X.509 certificates using TLS as defined in the 3GPP TS 33.310 [8] and independently verify the validity of each other's certificate, see Figure 5.0 below.

****

Figure 5.0 - Authentication Procedure

The authentication is performed based on standard (D)TLS connection and certificate exchange. Authorization may be performed prior to any transaction to allow the BM-SC to check the access rights of the content provider. Such authorization procedure, if successful, will result in the creation of an "access token" that the server will return to the content provider for subsequent requests made on the xMB interface.

## 5G Multicast Broadcast Services (MBS) architecture

To address broadcast/multicast requirements with 5G, different architecture had to be adopted. Therefore, the MBS architecture was defined as shown in Figure 6.0.

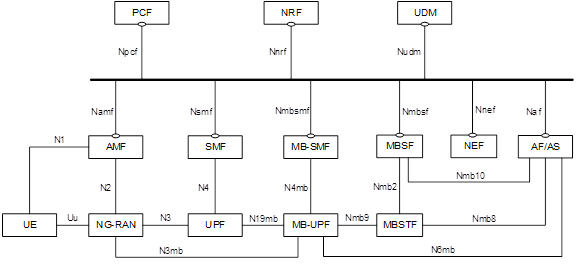


Figure 6.0 MBS architecture (3GPP [TS 23.247](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3854) v17.4.0)

As can be seen, the MBS related entities are within the 5G Core (5GC) and there are four entities that need to be deployed to support MBS:

* Multicast/Broadcast Session Management Function (MB-SMF): manages MBS sessions and interacts with the RAN and MB-UPF for data transport.
* Multicast/Broadcast User Plane Function (MB-UPF): enforces QoS and delivers multicast and broadcast to UPF or RAN nodes.
* Multicast/Broadcast Service Function (MBSF): provides service level functionality for MBS, including interaction with Application Function (AF) and MB-SMF for MBS sessions.
* Multicast/Broadcast Service Transport Function (MBSTF): provides generic packet transport functionalities and serves as media anchor for MBS data traffic.

Two delivery methods were defined to support MBS. First is the 5GC shared MBS traffic delivery method, where 5GC receives a single copy of MBS data packets and delivers a single copy of those MBS packets to a Next Generation RAN (NG-RAN) node, this is then delivered to one or multiple UEs. The second is 5GC Individual MBS traffic delivery method. This is where a single copy of MBS data packets received by 5GC is delivered as separate copies each to be delivered to an individual UEs via pe-UE Packet Data Unit (PDU) sessions. The difference is outlined in Figure 7.0. Note that the NG-RAN decides whether to transmit the MBS data packets in Point-to-Point (PTP) delivery method or Point-to-Multipoint (PTM) delivery method. Where the former delivers separate copies of MBS data packets over radio interface to each individual UE while the latter delivers a single copy of MBS data packets over radio interface to multiple UEs.

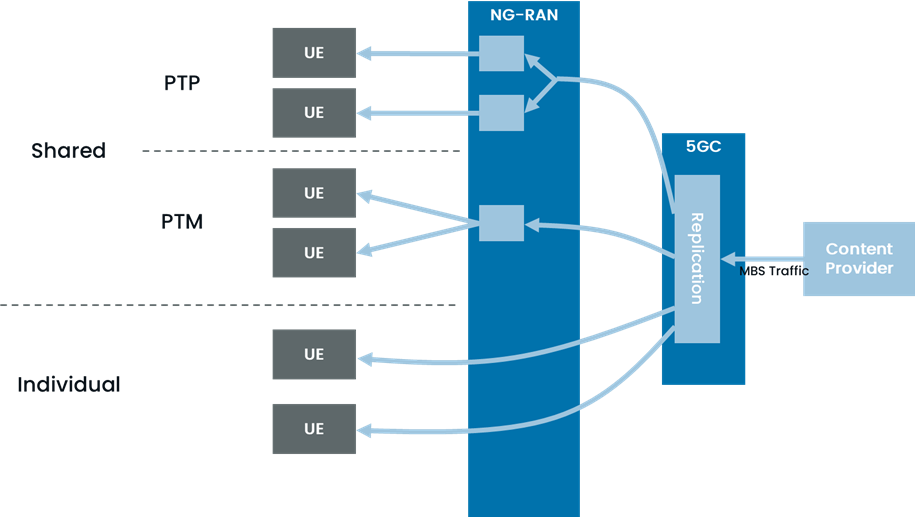


Figure 7.0 Delivery methods for MBS (3GPP [TS 23.247](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3854) v17.4.0)

To provide multicast/broadcast service, the MBS service is broken down into different phases (also summarised in Figure 8.0).

* MBS session creation: The AF provides information necessary to create MBS session towards 5GC. Optional for multicast.
* Service announcement: distribute information toward UEs about the service required for service reception. Optional for multicast.
* (Multicast only) Session establishment: The multicast MBS session is established with the joining of the first UE.
  + For multicast, the UE may join or leave the session via UE Session Join/Leave phases.
* (Multicast only) No data receiving: No data is received by 5GC. Optional for multicast.
* Data transfer: Multicast/broadcast data are transferred to the UEs
* (Multicast only) Session release: The multicast MBS session is released with the last UE leaving.
  + For multicast, the UE may join or leave the session via UE Session Join/Leave phases.
* (Multicast only) Session deletion: The multicast MBS session is deleted, with all information related to the session being removed from 5GC.
* (Broadcast only) Session release & deletion: The resources for the broadcast MBS session in 5GS are released and the broadcast MBS session is deleted.

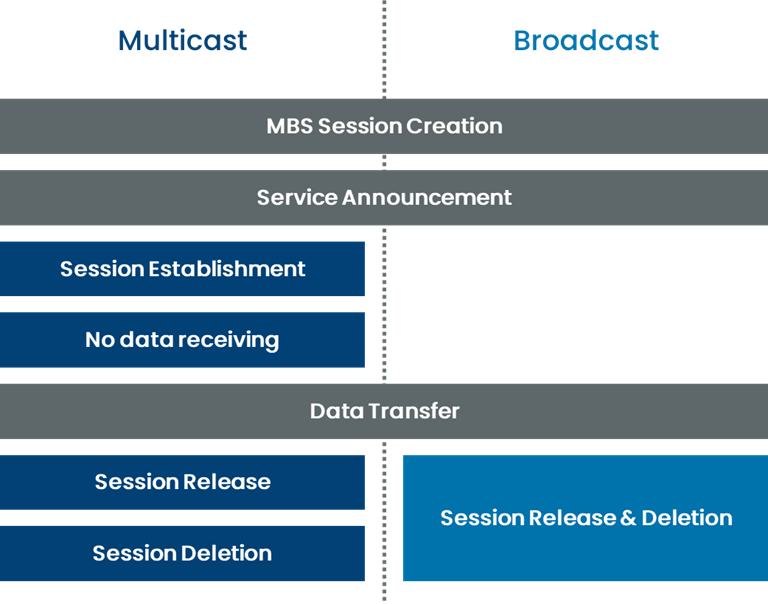


Figure 8.0 Data provisioning phases for MBS services (3GPP [TS 23.247](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3854) v17.4.0)

# Threat Analysis

This section based on the European Union Agency for Network and Information Security (ENISA) reports. As shown in Figure 9.0 below (borrowed from ENISA report on 5G threats [1]), ISO 27005, a widely adopted risk management standard, defines that risks emerge when threats become attacks that abuse vulnerabilities of assets to generate harm for the organisation. This methodology is a good approach in identifying threats to 5G networks with eMBMS/MBS elements. A more detailed threats map is shown in Appendix B.1and the security assurance methodology is presented in Appendix B2.

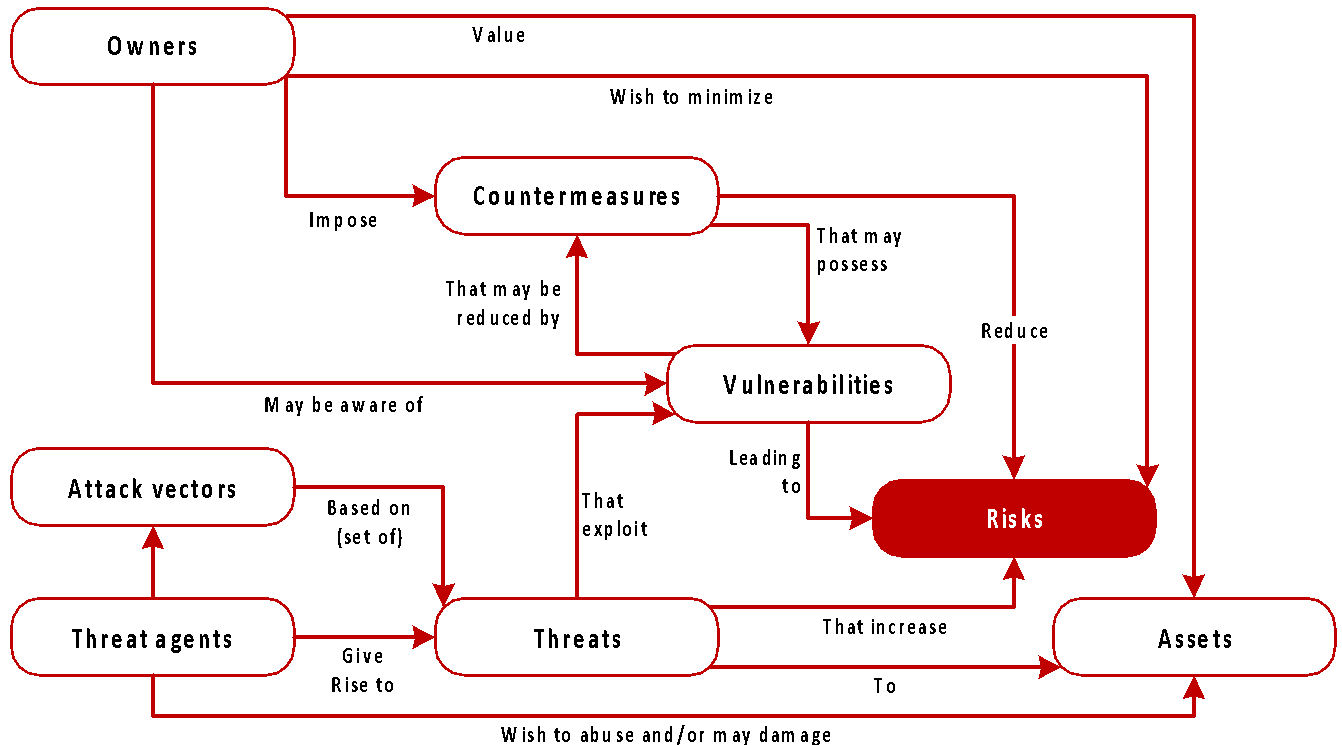


Figure 9.0 - Methodology adopted based on ISO 27005 [ENISA report on 5G threats]

Here is a taxonomy of high-level threat categories in 5G ONE4HDD:

* Nefarious activity/abuse (NAA): This threat category is defined as “intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target”.
* Eavesdropping/Interception/ Hijacking (EIH): This threat category is defined as “actions aiming to listen, interrupt, or seize control of a third-party communication without consent”.
* Physical attacks (PA) and the related Damage (DAM) or Failures or malfunctions (FM).

In relation to 5G network and in addition to the above general taxonomy, it is possible to categorise threats depending on whether the exploitation target is part of the core network, the radio access network or a generic infrastructure component. Based on this criterion, threats can be further categorised into:

* Generic threats: These are threats that typically affect any ICT system or network such as Denial of Service (DoS) threat.
* Core Network threats: These threats relate to elements of the Core Network that includes SDN, Network Function Virtualization (NVF), Network Slice (NS) and Management and orchestration (MANO). The majority fall under the categories of ‘Nefarious activity/abuse’ and ‘Eavesdropping/ Interception/ Hijacking’.
* Access network threats: These threats relate to the 5G radio access technology (RAT), Open Radio Access Network (ORAN) and non-3GPP access technologies. These include threats related to the wireless medium and radio transmission technology. The majority of the threats fall under the categories of ‘Eavesdropping/Interception/ Hijacking’.
* Multi-edge computing (MEC) threats: These threats relate to components located at the edge of the network. The majority fall under the categories of ‘Nefarious activity/abuse’ and ‘Eavesdropping/ Interception/ Hijacking’.
* Physical Infrastructure threats: These are threats related to the underlying IT infrastructure that supports the network. The majority fall under the categories of ‘Equipment failures or malfunctions’ or ‘Damage or loss of equipment’.
* Management threats, including failure to maintain logs of events for detection of attacks, or accidental mistakes (by non-hostile actors) or deliberate mistakes introduced following successful attacks.

The threats listed above will, when they become exploits of vulnerabilities (attacks), are a subset of the wider threat landscape that we consider having highest impact and/or highest likelihood (i.e. security risk). A more detailed threat analysis for 5G networks is presented in Appendix B.1 and the security assurance methodology in B.2 and they will be used for guiding the future security development in this project.

Note: Figure 1.0 in section 2, shows the major components in 5G ONE4HDD. The following subsection analyses the threats to the major components such as 5G (generic), RAN/ORAN and MBMS threats.

## 5G Generic Threats

The generic 5G architecture with its main 5G architecture components depicted as labelled boxes are shown in Figure 10.0. Some of the possible threats to the 5G generic architecture that are relevant to 5G ONE4HDD are (note: some of the text below is taken from ENISA threat landscape for 5G Networks [1]):

* Denial of Service (DoS): DoS is a threat categorised under Nefarious Activity and Abuse of Asset (NAA), in which the perpetrator seeks to make a network resource unavailable to its intended users by temporarily or indefinitely interfering or disrupting the network service. An attack combining multiple vectors may lead to a Distributed DoS (DDoS) attack.
* Data breach, leak, theft destruction and manipulation of information: This includes, but not limited to, the theft of personal information through unauthorised access to the systems and/or network, unauthorised access to and possible publication of personal identifiable information/biometric/medical (privacy breach).
* Eavesdropping: Classified as Nefarious Activity and Abuse of Asset (NAA). It includes the eavesdropping on subscriber’ data, confidential information, system time, subscriber location, electronic messages, signal of data relayed over the network.
* Exploitation of software and hardware vulnerabilities: This type of threat enables a malicious actor to take advantage of unknown (to the vendor and user) or unpatched software or hardware flaws to perform an attack. Examples include the exploitation of known hardware and software flaws such as meltdown and buffer overflow.
* Exploiting flaws in security, management and operational procedures: Not directly related with 5G, this threat will become relevant when dealing with the complexity of the technology and the need to introduce operational procedures to the management of the Network.
* Identity theft or spoofing: This threat may materialise when a malicious actor successfully determines the identity of a legitimate entity and then masquerades to launch further attacks.

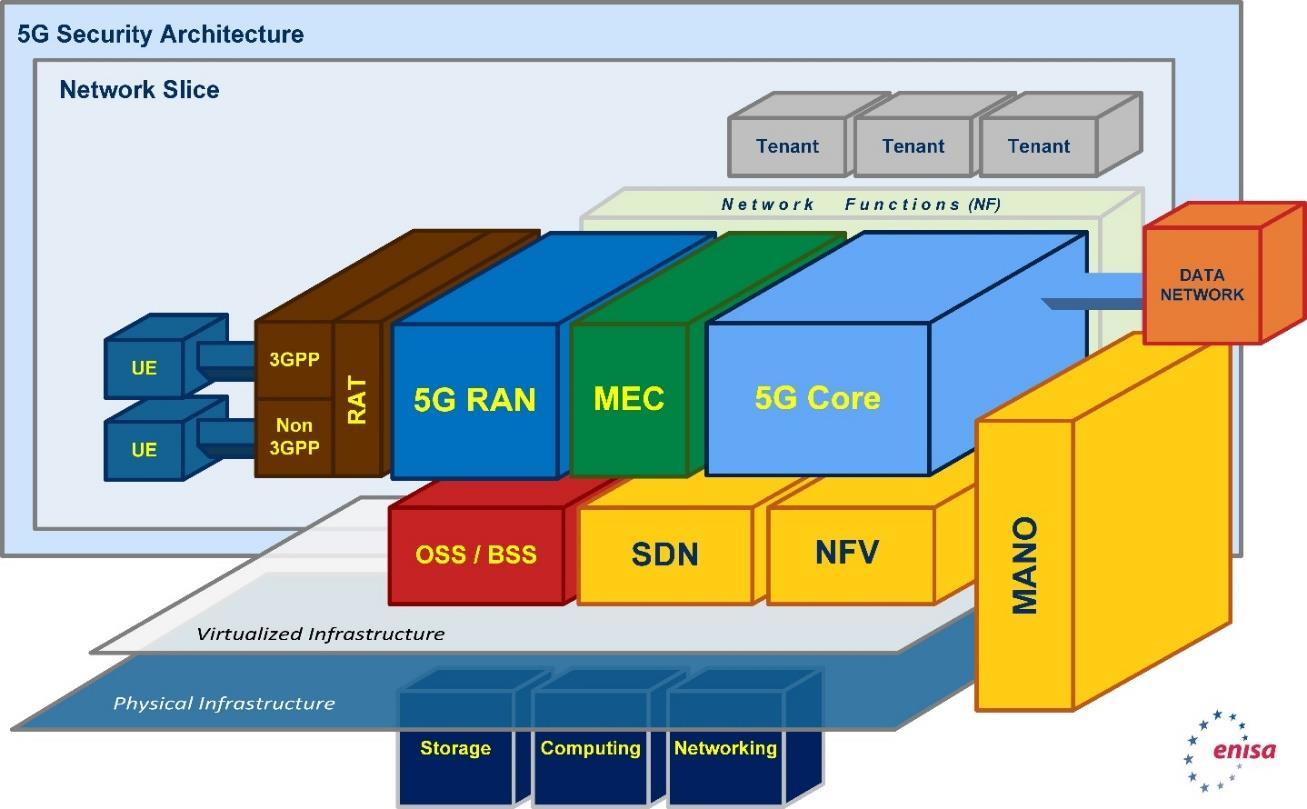


Figure 10.0 - 5G High-level generic architecture [ENISA report on 5G threats]

## Open Radio Access Network (ORAN) Threats

* Abuse of spectrum resources: The illegal use of these resources, due to the dynamic allocation/ reallocation of the same, may allow the occupation of a specific idle spectrum band by imitating the characteristics of a legitimately licensed unit and causing interference in radio frequencies..
* Fake access network node: Classified as a nefarious activity, this threat considers the compromise of a base station (gNB) by masquerading as legitimate, facilitating different types of attacks such as man-in-the-middle or network traffic manipulation.
* Flooding attack: This threat involves flooding radio interfaces with requests. Flooding occurs through the transmission of data that can exhaust component resources and lead to a reduction or complete shutdown of the radio frequency provided by the component.
* IMSI (or SUPI) catching attacks: The user identity uses the International Mobile Subscriber Identity (IMSI) in earlier generations of mobile networks, or the Subscription Permanent identifier (SUPI) in 4G/5G. This threat relates to cellular paging protocols that can be exploited by a malicious actor in the vicinity of a victim to associate the victim’s soft identity (e.g., phone number, Twitter handle).
* Jamming the radio frequency: Classified as a nefarious activity/abuse of asset, this threat refers to an intentional disruption/interference of the network radio frequency causing the core network (and related services) to become unreachable for affected users.
* Manipulation of access network configuration data: This threat involves compromising an access network element (e.g., base stations) to forge configuration data and launch other attacks (e.g. DoS).
* Session hijacking: This threat is classified as nefarious activity or abuse of asset and relates to attacks to open-air interfaces. The threat considers the theft of legitimate authenticated conversation session ID by a malicious actor, to control the whole session of specific traffic to conduct other types of attacks.
* Signalling storms: Mobile networks are subject to ‘signalling storms’ launched by malware or apps, which overload the bandwidth at the cell, the backbone signalling servers, and Cloud servers, and may also deplete the battery power of mobile devices.

There are other ORAN specific threats such as:

* ORAN interface threat: Opening up interfaces in the RAN network allows third-party applications to access information flows, which creates new security risks related to data passing through the network.
* ORAN protocol stack threat: In ORAN architecture, the radio stack breaks up into separate components as radio unit (RU), distributed unit (DU), and central unit (CU), which may be supplied by different vendors, this may pose a challenge to ensuring security and integrity in the RAN system is ensured, considering operations and management of RAN systems.
* Open-source RAN software threat: As the Open RAN technology evolves, the use of open-source software is expected to become increasingly prevalent. However, this brings forth new security challenges related to maintaining a consistent and comprehensive security approach to design, as well as preventing the introduction of deliberate security flaws.
* Multi-vendor RAN environment threat: In multi-vendor environment is it difficult to coordinate security policies and determine responsibility for security problems and requires more effective network security monitoring capabilities.

## Multi-access Edge Computing (MEC) Threats

MEC (Multi-access Edge Computing) used for the provision of cloud computing capabilities at the edge of the network, that is, for high bandwidth, low latency end user applications. MEC is located in the logical vicinity of base stations through authorised third parties willing to offer processing and storage capabilities to subscribers of the 5G network (ETSI ISG MEC white paper on MEC security [12]). This MEC environment is characterized by a complex multi-vendor, multi-supplier, multi-stakeholder ecosystem of equipment including both HW and SW devices. Given this overall level of system heterogeneity, areas of security, trust, and privacy are key topics for the edge environments.

This environment requires tackling MEC security with an end-to-end (E2E) approach, by leveraging existing standards relevant in the area, as carefully selected to be applicable in edge computing systems. Figure 11.0 shows the MEC high-level architecture.

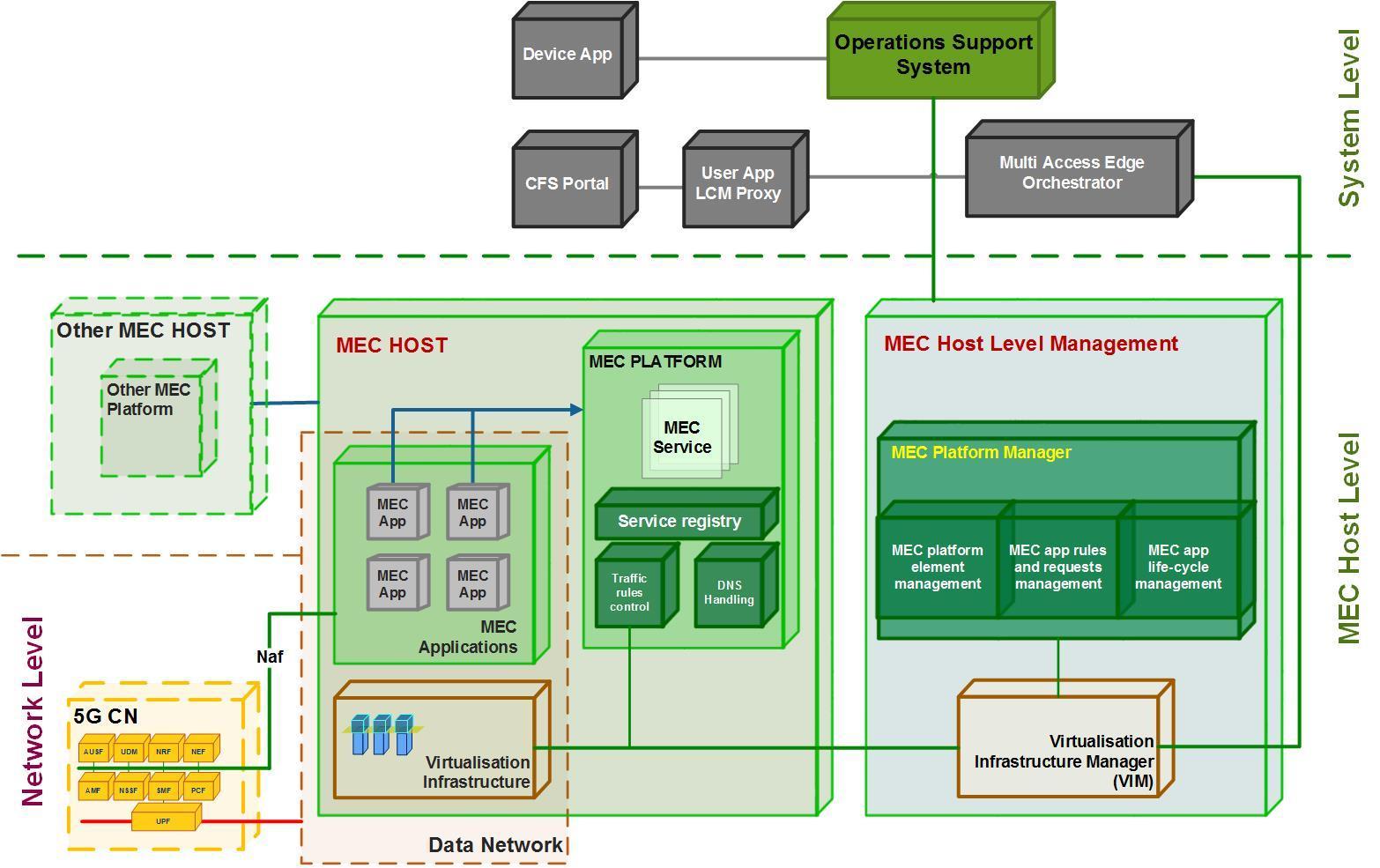


Figure 11.0 - 5G MEC high-level architecture [ENISA report on 5G threats]

Here is a list of possible threat to the MEC that are relevant to 5G ONE4HDD:

* False or rogue MEC gateway: The open nature of edge gateways, where even user-owned devices can become full-fledged participants (e.g. personal cloudlets, TV smart-box, etc.), creates a scenario where malicious actors can deploy their own gateway devices. This particular threat produces the same outcome as the Man-in-the-Middle attack.
* Edge node overload: This threat relates to attacks against edge networks disrupting the vicinity of the affected networks, at a local or service-specific level. The overload may take place by flooding the edge node with request or traffic directed to this component, initiated by a specific mobile app or IoT device.
* Abuse of edge open Application Programming Interfaces (APIs): The abuse of open APIs in MEC nodes is done through the exploitation of vulnerabilities in MEC type of applications. The need for open APIs in MEC is mainly to provide support for federated services and interactions with different providers and content creators. This threat can be associated with DoS, Man-in-the-Middle, malicious mode problems, privacy leakages, and Virtual Machine (VM) manipulation.

## Multicasting using eMBMS/MBS threats

In this section, we analyse the security threat for eMBMS/MBS. Starting with the trust model recommended by (3GPP TS 33.246 on MBMS security [9]) and the MBS has a similar trust model.

The following trust relationship between the roles that are participating in eMBMS services are proposed:

- The user trusts the home network operator to provide the eMBMS service according to the service level agreement.

- The user trusts the network operator after mutual authentication.

- The network trusts an authenticated user using integrity protection and encryption at RAN level.

- The network may have trust or no trust in a content provider.

The home network and visited network trust each other when a roaming agreement is defined, in the case the user is roaming in a VPLMN (Visited Public Land Mobile Network).

The threats to eMBMS (and MBS) system can be split into the following categories:

- Unauthorised access to eMBMS User data: such as intruders may eavesdrop eMBMS User data on the air-interface; Users that have not joined and activated a MBMS User Service, receiving that data without being charged; Users that have joined and then left a eMBMS User Service continuing to receive the eMBMS User data without being charged; or Valid subscribers may derive decryption keys and distribute them to unauthorised parties (insider attack).

- Unauthorised access to eMBMS User Services: An attacker using the 3GPP network to gain "free access" of MBMS User Services and other services on another user's bill without any knowledge of the service provider.

- Threats to integrity: This covers modifications and replay of messages, e.g. replace the actual content with a fake one.

- Denial of Service (DoS): Such as jamming of radio resources or deliberate manipulation of the data to disrupt the communications.

# Security Requirement

Note: some security requirements are expressed explicitly as mandatory implementation of specific standards. Others are expressed in terms of capabilities to detect, protect against, or recover from attacks.

## Security Requirements for 4G/5G ORAN and Core

From the threat analysis in section 3 and in relation to the 5G ONE4HDD 4G/5G network, the following requirements are derived:

1. User data and signalling data confidentiality and integrity: In the context of 5G, the gNB should support ciphering of user data between the UE and the gNB. Also, the gNB should support ciphering and integrity protection of user data, based on the security policy sent by the Session Management Function (SMF). In addition, the gNB should support ciphering and integrity protection of RRC-signalling.
2. Requirement for the gNB setup and configuration: Setting up and configuring gNBs by O&M systems should be authenticated and authorised by gNB so that attackers shall not be able to modify the gNB settings and software configurations via local or remote access.
3. Requirement for the gNB F1 and E1 interfaces: As stated in [3], gNBs with split DU-CU implementations should support confidentiality, integrity and anti-replay protection.
4. Requirement for secure xApp/rApp application deployment: Adequate, flexible and verifiable technical measures need to be implemented to ensure a secure and trustworthy xApp/rApp deployment on the RIC platform. It needs a mandatory inclusion of authentication and authorization within the xApp onboarding, provisioning, and registration processes.
5. Ensuring strict access to shared data: The RIC management and orchestration platforms have databases which contain sensitive UE and ORAN information, including the history of the network state, configurations related to E2 Nodes, cells, bearers, flows, UE identities, and the mappings between them. Access to this information needs to be protected and authorised.
6. Requirement on the Core network security: The 3GPP specification in TS 33.501 [10], assumes that mobile network operators subdivide their networks into trust zones. Messages that traverse trust boundaries (roaming) should follow the requirements in service-based architecture (sub-clause 5.9.2).

All the above network ORAN/Core requirements could be satisfied by following the ORAN Alliance and 3GPP security specifications TS 33.501 [10].

## Security Requirements for MEC

From the threat analysis in section 3 and in relation 5G ONE4HDD 4G/5G network, the following MEC requirements are derived:

1. Considering 5G ONE4HDD real time video streaming, the TLS/DTLS should also be supported by the MEC, enabling a MEC to securely connect multiple cameras using TCP or UDP. This also includes secure connectivity between the MEC and MB-SC (or MBSTF in MBS).
2. The major security emphasis in MEC specifications is on securing access to MEC service APIs by service consuming applications. ETSI ISG MEC standardises a variety of MEC services by specifying implementation agnostic, RESTful APIs using HTTP. ETSI GS MEC 009 mandates support for HTTP over TLS (also known as HTTPS) using TLS version 1.2 (as defined by IETF RFC 5246). TLS version 1.3, defined by [IETF RFC 8446], should be also supported.
3. Network Function Virtualization (NFV) and MEC security requirements are complementary concepts: for example one of the main MEC components at host level is the virtualization infrastructure, which provides compute, storage, and network resources for the MEC Applications. The NFV Security WG (NFV SEC) has concentrated on analysing threats to security in virtualized environments and published a series of specifications and reports on security requirements and solutions for NFV in the past few years.

## Security Requirements for eMBMS/MBS

From the above threat analysis in section 3 and in relation to 5G ONE4HDD, the following requirements are derived:

1. End-to-end confidentiality and integrity protection of user data such using DTLS between content provider and a group of UEs.
2. MB-SC (or MBSTF in MBS) unicast connection to the MEC should be confidentiality and integrity protected using TLS.
3. Requirements on secure service access: A valid USIM or SIM is required to access eMBMS/MBS User Services. Also, it should be possible to prevent intruders from obtaining unauthorised access of eMBMS/MBS User Services by masquerading as authorised users.
4. Requirements on secure service provision: It should be possible for the eMBMS network (i.e. BM-SC (or MBSTF in MBS) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorised access to eMBMS/MBS User Services. Also it should be possible to prevent the use of a particular USIM or SIM to access eMBMS/MBS User Services.
5. Requirements on eMBMS/MBS Key Management: The transfer of the eMBMS/MBS keys between the eMBMS/MBS key generator and the UE should be confidentiality and integrity protected.
6. Requirements on eMBMS/MBS re-Keying policy: to ensure that past users who have left the system do not gain further access to the eMBMS/MBS User Services. Also new users joining an eMBMS/MBS User Service will not gain access to past (historical) data from previous transmissions. This is sometimes referred to as forward and backward security.

# Security Recommendations

Examining the security threat in section 3 and the security requirement in section 4, the following security recommendations are derived:

1. Regarding the mobile network core and ORAN, implementing the 3GPP security specifications such as TS 33.501 [10] should be sufficient, provided that optional features are implemented consistently, be adequate to satisfy the security requirements in section 4.1, such as UE and network authentication and authorisation plus data and signalling confidentiality and integrity protection. In ONE4HDD, the VMO2 mobile network follows (broadly) these standards and there is no usage of High-Risk Vendors (HRVs).
2. Regarding the MEC and eMBMS/MBS protection and in relation to the 5G ONE4HDD real time video streaming, using DTLS/TLS is recommended between the MEC and content providers (including the cameras in the 5G ONE4HDD system). Also TLS is recommended for the connection between MEC and MB-SC (or MBSTF in MBS). This will provide access control (authentications and authorisation) plus confidentiality and integrity protection for user data. Optional security is also possible for other unicast hops in the network such as using TLS between content provider (e.g. cameras) and the MEC.
3. In relation to the secure broadcasting/multicasting that was discussed in section 1, DTLS is recommended as an end-to-end application layer solution between the Content Provider and a group of UEs.
4. Regarding key management, the use of a flat-key system (see Section 1) is recommended for static and small groups (fixed membership) and LKH is recommended for dynamic and large groups (changing membership).

Regarding the choice of DTLS as a security system, further justifications for this choice include:

* DTLS works with UDP and fits very well with secure group communications. It is also recommended in the 3GPP TS 33.246 [5]. Hence and in 5G ONE4HDD, DTLS will be used to secure the end-to-end multicasting.
* Also DTLS is a suitable system to secure the unicast or multicast connection between the MB-SC and MEC. This will provide protection against spoofing, DoS, DDoS, Man-in-the-Middle attacks, etc.
* Similar to the MB-SC (or MBSTF)-MEC arrangement, DTLS is a suitable system to secure the unicast or multicast connection between the MEC and Content Providers.

Finally, providing end-to-end security (application layer) using DTLS and LKH will scale well and is agnostic to the RAN/ORAN technologies. It can also bridge the security gaps between MNO and Broadcast Network Operators (BNO).

# Next Steps

## Simplified ONE4HDD security architecture

Based on the security analyses in sections 3 and 4 and the recommendations in section 5, and at this early stage of the ONE4HDD project, Figure 12.0 below shows a simplified security architecture for ONE4HDD. More elaborate security architecture will be defined at the later stages of the project.

The work will start with a more detailed threat Analysis to the architectural elements of ONE4HDD such as ORAN (or similar technologies that will be adopted in ONE4HDD) plus the users and content providers.

The security strategy first step is focused on the unicast security between the MEC and Scheduler and Broadcast Controller using techniques such as Transport Layer Security (TLS). The justification for such security is to ensure the authentication and authorisation of the streaming data entering the network. This is critical for multicast and broadcast service. The aim here is to comply with the security recommendations in section 5 in relation to mutual authentication, authorisation plus user-data and signalling-data confidentiality and integrity.

A diagram of a network

Description automatically generated

Figure 12.0 – Simplified Security architecture for ONE4HDD

Also and in relation to the HDD challenging environment, the second step is the Multicast security design Proof of concept using simulation demo for securing 5G ONE4HDD end-to-end user traffic, as shown the Figure 12.0. The work here is focused on providing end-to-end multicast security to protect content and users’ data and identities in HDD. The justification for this strategy is that the eMBMS/MBS components and security procedure are not fully realised in real systems. Therefore, the end-to-end security approach will provide protection irrespective of the underlying technologies.

As such by combining unicast and multicast security full protection will be provided to the 5G ONE4HDD system and stakeholders.

## security research and development areas

The security research will focus on secure multicasting and broadcasting. Looking ahead towards 6G, secure multicasting/broadcasting will need to be dynamic and scalable for large groups that could be distributed in wide areas. This might include 3D networks (including satellites, Drones and High Altitude Platforms, HAPS).

The ONE4HDD research is focused on using Logical Key Hierarchy (LKH), as described in section 1. LKH will be a key enabler for scalability of the ONE4HDD use cases. This research will also cater for future use cases where multicast groups could span large geographic areas (e.g. multicast users are spread through several major cities, like a popular football game) and multiple administrative domains (e.g. multiple mobile operators and cloud providers).

Finally, this document has been developed to follow the principles outlined by DSIT in their recommendations for the ONE Programme - Security Strategy (in the FGA). Broadly speaking, all the relevant topics in the list of priority security research and development areas in the FGA are covered in this deliverable.

This includes a list of topics to be addressed:

* Technical description of the system and its assets – to do.
* Threat assessment – top level done. More detailed analysis to do.
* Risk assessment –relying on analyses done by ENISA and others. However, top level assessment and assurance is done
* Mitigating measures – to do.
* Implementation plan – to do.
* Ongoing assessment – to plan.

The latter two items will be the focus of through-life security maintenance of the 5G ONE4HDD system.

# Annex A - Acronyms

|  |  |
| --- | --- |
| 5G-PPP | 5G Public Private Partnership |
| 3GPP | 3rd Generation Partnership Project |
| API | Application programming interface |
| ARP | Address resolution protocol |
| AS | Access stratum |
| BM-SC | Broadcast multicast service centre |
| BNO | Broadcast Network Operator |
| CN | Core network |
| DoS | Denial of Service |
| DDoS | Distributed DoS |
| DTLS | Datagram Transport Layer Security |
| DVB | Digital video Broadcasting |
| EIH | Eavesdropping/Interception/ Hijacking |
| eMBB | enhanced mobile broadband |
| ENISA | European Union Agency for Network and Information Security |
| ETSI | European Telecommunications Standards Institute |
| eMBMS | enhanced Multimedia Broadcast Multicast Service |
| gNB | Base station |
| HRV | High Risk Vendors |
| IP | Internet protocol |
| IETF | Internet Engineering Task Force |
| MAC | Media Access Control |
| MANO | Management and orchestration |
| MBMS | Multimedia Broadcast Multicast Service |
| MBMS-GW | MBMS gateway |
| MCPTT | Mission Critical Push to Talk |
| MCE | Multi-cell/multicast coordination entity |
| MEC | Multi-access edge computing |
| mMTC | Massive machine-type communication |
| MNO | Mobile network operator |
| MTC | Machine Type Communications |
| NAA | Nefarious activity/abuse |
| NAS | Non-Access Stratum |
| NIC | Network Interface Controller |
| NFV | Network Function Virtualization |
| NS | Network slice |
| ORAN | Open Radio Access Network |
| PLMN | Public Land Mobile Network |
| RAN | Radio Access Network |
| RAN-CU | RAN Centralised unit |
| RAT | Radio Access Technology |
| SDN | Software defined network |
| SUCI | Subscription concealed identifier |
| SUPI | Subscription Permanent identifier |
| TCP | Transport control Protocol |
| TLS | Transport Layer Security |
| TSoIP | Transport Stream over IP |
| UDP | User Datagram Protocol |
| UE | User equipment |
| URLLC | Ultra-reliable low-latency communication |
| USIM | Universal subscriber identity module |
| VM | Virtual Machine |
| VPLMN | Visited PLMN |

# Appendix B: 5G Threat Map and security assurance

## B.1 5G Threat Map

The threat map for 5G technologies as defined by the European Union Agency for Cybersecurity, [13] is shown in Figure 29.



Figure 13.0 – Threat map for 5G Technologies

## B.2 The 3GPP Security assurance Methodology (SECAM)

The security assurance process describes how the operator gets assurance regarding the security of the network product [3GPP TR33.916]. The process is depicted in Figure 14.0 [14]. If there are any regulatory requirements on security assurance of the network product, they will for the purpose of this process model be considered being included in the acceptance requirements of the operator.

When a vendor is ready to provide security assurance w.r.t. a given network product, the vendor obtains one or more Security Assurance Specifications that the network product is aiming to fulfil. Choice of which SCASs to select may depend on operator and/or regulatory input. Then the product is evaluated against the Security Assurance Specification(s).

Once the operator received the evaluation report, the operator then decides if the results are sufficient according to its internal policies and whether to accept the security assurance level of the network product or not. The operator's acceptance decision may depend on external forces such as regulatory requirements.



Figure 14.0 - SECAM defined Security assurance process

# Appendix C: ONE4HDD IP ARRANGEMENT

1. Project activities relating to IPR

* Training researchers in the field of IPR
* What is a patent
* How to search existing patents
* What is the potential value of a patent
* When/why to file IPR vs. publishing vs. keeping confidential
* What makes a good patent proposal
* Pre-project creation of a legal framework for handling of project partners’ background IPR brought into the project and new IPR generated by partners, as part of the Consortium Agreement. This addresses issues such as:
* Ownership of Background IPR
* Ownership of any Background IPRs remains with owning party.
* Access rights to background IPR, for use within the project
* Background IPRs (subject to any existing obligations to third parties) are licenced for the purpose of undertaking the Project and to enable the use of the Developed IPRs under clause, but not for commercial exploitation unless agreed.
* Access rights to IPR generated within the project, for use within the project
* Access rights to IPR used within the project for future exploitation of project results outside the project
* If any Party wishes to commercially exploit Developed IPRs owned by another Party if such developed IPRS are needed, the Parties concerned will enter into good faith commercial discussions to agree on the terms of a non-exclusive licence to use the Developed IPRs, including a royalty and/or other appropriate form of remuneration which is fair and reasonable
* Timely declaration of IPR generated within the project
* Maintaining a record of IPR generated within the project via project board
* Propose potential exploitation routes for TUDOR innovations via project board

2. Ownership and Management of project related IPR

Developed IPRs will vest on creation in the Party that developed the Developed IPRs

In relation to the Protection of Developed IPRs:

Each Party has agreed that, for the Term and for six months thereafter to undertake and continue at its expense the timely Protection of Developed IPRs that it owns; it is agreed, however, that a Party may decide that it is suitable for it to put part of its Results under an open-source license subject to the agreement of any joint owners.

If a party does not wish to continue to protect, the Project Board will be notified as soon as possible and the Project Board will decide how best to Protect those Developed IPRs, which may include recommending an assignment of the Developed IPRs to another Party.

In order to maximise the partners’ ability to effectively exploit IPR in standards and for development of the UK economy the industrial partners have a strong preference that IPR generated within the project shall be owned by the partner who creates them. Yes as above

How to handle IPR jointly created by more than one partner:

Joint owners of Developed IPRs will agree between them on who will be responsible for the Protection of the jointly owned Developed IPRs and the nominated Party or Parties may charge the other joint owners for the actual costs of Protection as agreed between the joint owners and in the absence of any agreement, the costs will be shared between the owners according to their ownership interest in the Developed IPRs.

# REFERENCES

1. The European Union Agency for Cybersecurity (ENISA), “ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Threat assessment for the fifth generation of mobile telecommunications networks (5G)”, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks , Nov 2019.
2. Rohde& Shwarz report,“5G BROADCAST/MULTICAST, Redefining the future of content delivery” <https://www.rohde-schwarz.com/ch/loesungen/broadcast-and-media/content-distribution/terrestrial-transmission/5g-broadcast/5g-broadcast_250909.html>
3. 5G ONE4HDD HDL report: <https://drive.google.com/drive/folders/1hcnkWrJi59q_1uJl_BRV0n1UhsM1Me4a>
4. 3GPP TS 23.246 V16.1.0 (2019-09): <https://www.3gpp.org/ftp/Specs/archive/23_series/23.246/>
5. 3GPP TS 26.346 V16.9.1 (2021-05):<https://www.etsi.org/deliver/etsi_ts/126300_126399/126346/16.09.01_60/ts_126346v160901p.pdf>
6. 3GPP TS 26.348 V16.3.0 (2020-03): <https://www.3gpp.org/ftp/Specs/archive/26_series/26.348/>
7. R&S BSCC product specifications: <https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/BSCC2_bro_3608-1846-12_v0200.pdf>
8. 3GPP TS 33.310: <https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/>
9. 3GPP TS 33.246: <https://www.3gpp.org/ftp/Specs/archive/33_series/33.246/>
10. 3GPP TS 33.501: <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/>
11. 3GPP TS 33.220: <https://www.3gpp.org/ftp/Specs/archive/33_series/33.220/>
12. ETSI ISG MEC white paper on MEC security: <https://www.etsi.org/newsroom/press-releases/1933-etsi-releases-a-white-paper-on-edge-computing-security>
13. The European Union Agency for Cybersecurity (ENISA), “ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Updated hreat assessment for the fifth generation of mobile telecommunications networks (5G)”, Dec 2020: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks>
14. 3GPP TR 33.916, Security Assurance Methodology (SECAM) for 3GPP network products

[end of document]