**3GPP TSG-SA3 Meeting #109 *S3-224169***

**Toulouse, France 14 - 18 November 2022** *revision of S3-223342*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **DRAFT** | **rev** |  | **Current version:** | **17.5.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network | **x** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Draft CR: Introducing split gNBs into TR 33.926 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-07-14 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-18 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Split gNBs are not covered. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Introduce the text for split gNBs text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Split gNB work will not be completed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, Annex W (new), Annex X (new), Annex Y(new), Annex Z (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | S3-222322 – baseline draft CR from SA3#108-e  S3-223342 – Updates S3-222322 with basetext from v17.5.0 of TR and makes a few editorials (add a newline and correct heading formats)  S3-224169 – Updates S3-223342 with S3-223343, S3-223344 and S3-223345 | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

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

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

[6] 3GPP TS 33.511: "5G Security Assurance Specification (SCAS); NR Node B (gNB)"

[7] 3GPP TS 38.300 v15: "NR; NR and NR-RAN Overall Description; Stage 2".

[8] 3GPP TS 23.501 v15: "System Architecture for 5G System; Stage 2".

[9] 3GPP TS 38.323 v15: "NR; Packet Data Convergence Protocol (PDCP) specification".

[10] 3GPP TS 38.322 v15: "NR; Radio Link Control (RLC) protocol specification".

[11] 3GPP TS 33.250: "Security assurance specification for the PGW network product class".

[12] 3GPP TS 33.516: "5G Security Assurance Specification (SCAS) for the AUSF network product class".

[13] 3GPP TS 33.517: "5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class".

[14] 3GPP TS 33.501 Release 15: "Security architecture and procedures for 5G system".

[15] 3GPP TS 33.518: "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class".

[16] 3GPP TS 33.519: "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class".

[17] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[18] 3GPP TS 33.513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description;Stage 2."

[20] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class."

[21] 3GPP TS 33.514: "5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class".

[22] 3GPP TS 33.512: "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)".

[23] 3GPP TS 33.521: "Security Assurance Specification (SCAS) for the Network Data Analytics Function (NWDAF) network product class".

[24] 3GPP TS 23.288: " Architecture enhancements for 5G System (5GS) to support network data analytics services".

[25] 3GPP TS 33.226: "Security assurance for IP Multimedia Subsystem (IMS)".

[26] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

[27] 3GPP TS 33.522: "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)".

[28] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 16).

[aa] 3GPP TS 38.300: "NR; NR and NR-RAN Overall Description; Stage 2" (Release 17).

[bb] 3GPP TS 38.401: "NG-RAN; Architecture description" (Release 17).

[cc] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 17).

[dd] 3GPP TS 33.742: "5G Security Assurance Specification (SCAS); Split gNB product classes".

**\*\*\*\* NEXT CHANGE \*\*\*\***

Annex W:   
Aspects specific to the network product class gNB-CU

# W.1 Network product class description for the gNB-CU

## W.1.1 Introduction

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

## W.1.2 Minimum set of functions defining the gNB-CU network product class

As part of the gNB-CU network product, it is expected that the gNB-CU contains gNB-CU application, a set of running processes (typically more than one) executing the software package for the gNB-CU functions and OAM functions that are specific to the gNB-CU network product model. Functionalities specific to the gNB-CU network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.742 [dd].

NOTE: For the purposes of the present document, this common set is defined to be the list of gNB-CU functions contained in 3GPP TS 38.300 [aa], 3GPP TS 38.401 [bb] and TS 23.501 [cc].

# W.2 Assets and threats specific to the CU

## W.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the gNB-CU to be protected are:

- gNB-CU Application;

- Mobility Management data: e.g. subscriber's identities (e.g. SUCI, GUTI), subscriber keys (i.e. KUPenc, KUPint, KRRCenc, KRRCint, NH), authentication parameters, APN name, data related to mobility management like UE measurements, UE's IP address, etc., QoS and so on, etc;

- User plane data;

- The interfaces of gNB-CU whose data is to be protected and which are within SCAS scope;

- N2 interface;

- Xn interface;

- N3 interface;

- Uu interface;

- F1 interface;

- Console interface, for local access: local interface on gNB-CU; and

- OAM interface, for remote access: interface between gNB-CU and OAM system; and

NOTE 1: The detailed interfaces of the gNB-CU class are described in clause 4, Network Product Class Description of the present document.

- gNB-CU Software: binary code or executable code.

NOTE 2: gNB-CU files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, gNB-CU application, Mobility Management data or gNB-CU Software.

## W.2.2 Threats related to Control plane and User plane in the network

### W.2.2.1 Control plane data confidentiality protection

- *Threat name*: gNB-CU control plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-CU does not provide confidentiality protection for control plane packets on the N2/Xn/F1-C/Uu reference points, then the control plane packets sent over Xn (e.g. inter-gNB handover), N2 (e.g. handover on AMF change), Uu and F1-C reference points can be compromised by attackers. This means the UE identifiers, security capabilities, the security algorithms and key materials exchanged can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the N2, Xn and F1-C reference points are not within the security environment.

- *Threatened Asset*: Mobility Management data.

### W.2.2.2 Control plane data integrity protection

- *Threat name*: Control plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-CU does not provide integrity protection for control plane packets on N2/Xn/F1-C/Uu reference points, the control plane packets sent over these reference points can be modified without detection. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the N2, Xn and F1-C reference points are not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data.

### W.2.2.3 User plane data confidentiality protection

- *Threat name*: User plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-CU does not cipher and decipher user plane packets on the N3/Xn/Uu/F1-U reference points, then the attackers can compromise user packets on F1-U, Uu, Xn-U and N3. The attackers can gain access to user identifiers, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the N3, F1-U and Xn reference points are not within the security environment.

- *Threatened Asset*: User plane data.

### W.2.2.4 User plane data integrity protection

- *Threat name*: User plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-CU does not handle integrity protection for user plane packets for the Xn/N3/Uu/F1-U reference points then all the uplink/downlink user plane packets can be manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the Xn, F1-U and N3 reference points are not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, User plane data.

### W.2.2.5 AS algorithm selection and use

- *Threat name*: AS algorithm selection and use

- *Threat Category*: Tampering data, Information Disclosure, Denial of Service

- *Threat Description*: If AS does not use the highest priority algorithm to protect AS layer, i.e. RRC and PDCP, data on the AS layer risks being exposed and/or modified, or denial of service.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data

### W.2.2.6 Bidding down on Xn-Handover

- *Threat name*: Bidding down on Xn-Handover.

- *Threat Category*: Tampering Data, Information Disclosure, Denial of Service.

- *Threat Description*: If the gNB-CU does not send the UE 5G security capabilities, the AMF cannot verify 5G security capabilities are the same as the UE security capabilities that the AMF has stored, the attacker may force the system to accept a weaker security algorithm than the system is allowed, forcing the system into a lowered security level making the system easily attacked and/or compromised.

- *Threatened Asset*: Sufficient processing capability, Mobility Management data.

### W.2.2.7 Key Reuse

- *Threat name*: Key Reuse.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If AS keys are not refreshed by the gNB-CU when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KgNB, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around.

- *Threatened Asset*: User plane data, Mobility Management data.

### W.2.2.8 Security Policy Enforcement

- *Threat name*: Security Policy Enforcement.

- *Threat Category*: Tampering data, Information Disclosure.

- *Threat Description*: If gNB-CU does not follow the security based on security policy provided by SMF, this can lead to no security or reduced security provided to the UE user plane, (e.g. not applying integrity protection when it is required to do so), etc.

- *Threatened Asset*: Sufficient Processing Capability, User plane data.

### W.2.2.9 State transition from inactive state to connected state

- *Threat name*: State transition from inactive state to connected state

- *Threat Category*: Denial of Service.

- *Threat Description*: When state transits from inactive state to the connected state, if the gNB-CU does not reactivate/activate the UP security based on UP activation status included in the UE 5G AS security context, the UP activation status between the network and the UE may be different. This will cause the misalignment on UP activation status, and result in the UE has to reconnect to the Network again which wastes resource both at UE and network

- *Threatened Asset*: Sufficient Processing Capability.

**\*\*\*\* NEXT CHANGE \*\*\*\***

Annex X:   
Aspects specific to the network product class gNB-CU-CP

# X.1 Network product class description for the gNB-CU-CP

## X.1.1 Introduction

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

## X.1.2 Minimum set of functions defining the gNB-CU-CP network product class

As part of the gNB-CU-CP network product, it is expected that the gNB-CU-CP contains gNB-CU-CP application, a set of running processes (typically more than one) executing the software package for the gNB-CU-CP functions and OAM functions that are specific to the gNB-CU-CP network product model. Functionalities specific to the gNB-CU-CP network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.742 [dd].

NOTE: For the purposes of the present document, this common set is defined to be the list of gNB-CU-CP functions contained in 3GPP TS 38.300 [aa], 3GPP TS 38.401 [bb] and TS 23.501 [cc]

# X.2 Assets and threats specific to the gNB-CU-CP

## X.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the gNB-CU-CP to be protected are:

- gNB-CU-CP Application;

- Mobility Management data: e.g. subscriber's identities (e.g. SUCI, GUTI), subscriber keys (i.e. KUPenc, KUPint, KRRCenc, KRRCint, NH), authentication parameters, APN name, data related to mobility management like UE measurements, UE's IP address, etc., QoS and so on, etc;

- The interfaces of gNB-CU-CP to be protected and which are within SCAS scope;

- N2 interface;

- Xn interface;

- E1 interface;

- Uu interface;

- F1 interface;

- Console interface, for local access: local interface on gNB-CU-CP; and

- OAM interface, for remote access: interface between gNB-CU-CP and OAM system; and

NOTE 1: The detailed interfaces of the gNB-CU-CP class are described in clause 4, Network Product Class Description of the present document.

- gNB-CU-CP Software: binary code or executable code.

NOTE 2: gNB-CU-CP files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, gNB-CU-CP application, Mobility Management data or gNB-CU-CP Software.

## X.2.2 Threats related to Control plane and User plane in the network

### X.2.2.1 Control plane data confidentiality protection

- *Threat name*: gNB-CU control plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-CU-CP does not provide confidentiality protection for control plane packets on the N2/Xn/F1-C/Uu/E1 reference points, then the control plane packets sent over Xn (e.g. inter-gNB handover), N2 (e.g. handover on AMF change), Uu, E1 and F1-C referemnce points can be compromised by attackers. This means the UE identifiers, security capabilities, the security algorithms and key materials exchanged can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the N2, Xn, E1 and F1-C reference points are not within the security environment.

- *Threatened Asset*: Mobility Management data.

### X.2.2.2 Control plane data integrity protection

- *Threat name*: Control plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-CU-CP does not provide integrity protection for control plane packets on N2/Xn/F1-C/Uu/E1 reference points, the control plane packets sent over these reference points can be modified without detection. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the N2, Xn, E1 and F1-C reference points are not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data.

### X.2.2.3 AS algorithm selection and use

- *Threat name*: AS algorithm selection and use

- *Threat Category*: Tampering data, Information Disclosure, Denial of Service

- *Threat Description*: If AS does not use the highest priority algorithm to protect AS layer, i.e. RRC and PDCP, data on the AS layer risks being exposed and/or modified, or denial of service.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data

### X.2.2.4 Bidding down on Xn-Handover

- *Threat name*: Bidding down on Xn-Handover.

- *Threat Category*: Tampering Data, Information Disclosure, Denial of Service.

- *Threat Description*: If the gNB-CU-CP does not send the UE 5G security capabilities, the AMF cannot verify 5G security capabilities are the same as the UE security capabilities that the AMF has stored, the attacker may force the system to accept a weaker security algorithm than the system is allowed, forcing the system into a lowered security level making the system easily attacked and/or compromised.

- *Threatened Asset*: Sufficient processing capability, Mobility Management data.

### X.2.2.5 Key Reuse

- *Threat name*: Key Reuse.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If AS keys are not refreshed by the gNB-CU-CP when PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same KgNB, key stream reuse is possible. This can result in information disclosure of AS signalling and user plane data. The threat of key stream reuse occurs under the following conditions when the PDCP COUNT is reset to 0 but the RB identity and key stay the same (e.g. the successive Radio Bearer establishment uses the same RB identity and keys, or the RB identity is increased after multiple calls and wraps around.

- *Threatened Asset*: User plane data, Mobility Management data.

### X.2.2.6 Security Policy Enforcement

- *Threat name*: Security Policy Enforcement.

- *Threat Category*: Tampering data, Information Disclosure.

- *Threat Description*: If gNB-CU-CP does not follow the security based on security policy provided by SMF, this can lead to no security or reduced security provided to the UE user plane, (e.g. not applying integrity protection when it is required to do so), etc.

- *Threatened Asset*: Sufficient Processing Capability, User plane data.

### X.2.2.7 State transition from inactive state to connected state

- *Threat name*: State transition from inactive state to connected state

- *Threat Category*: Denial of Service.

- *Threat Description*: When state transits from inactive state to the connected state, if the gNB-CU-CP does not reactivate/activate the UP security based on UP activation status included in the UE 5G AS security context, the UP activation status between the network and the UE may be different. This will cause the misalignment on UP activation status, and result in the UE has to reconnect to the Network again which wastes resource both at UE and network

- *Threatened Asset*: Sufficient Processing Capability.

**\*\*\*\* NEXT CHANGE \*\*\*\***

Annex Y:   
Aspects specific to the network product class gNB-CU-UP

# Y.1 Network product class description for the gNB-CU-UP

## Y.1.1 Introduction

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

## Y.1.2 Minimum set of functions defining the gNB-CU-UP network product class

As part of the gNB-CU-UP network product, it is expected that the gNB-CU-UP contains gNB-CU-UP application, a set of running processes (typically more than one) executing the software package for the gNB-CU-UP functions and OAM functions that are specific to the gNB-CU network product model. Functionalities specific to the gNB-CU-UP network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.742 [dd].

NOTE: For the purposes of the present document, this common set is defined to be the list of gNB-CU-UP functions contained in 3GPP TS 38.300 [aa], 3GPP TS 38.401 [bb] and TS 23.501 [cc].

# Y.2 Assets and threats specific to the gNB-CU-UP

## Y.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the gNB-CU-UP to be protected are:

- gNB-CU-UP Application;

- Mobility Management data: subscriber keys (i.e. KUPenc, KUPint), UE's IP address, etc., QoS and so on, etc;

- User plane data;

- The interfaces of gNB-CU-UP whose data needs to be protected and which are within SCAS scope;

- E1 interface;

- Xn interface;

- N3 interface;

- Uu interface;

- F1 interface;

- Console interface, for local access: local interface on gNB-CU-UP; and

- OAM interface, for remote access: interface between gNB-CU-UP and OAM system; and

NOTE 1: The detailed interfaces of the gNB-CU-UP class are described in clause 4, Network Product Class Description of the present document.

- gNB-CU-UP Software: binary code or executable code.

NOTE 2: gNB-CU-UP files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, gNB-CU-UP application, Mobility Management data or gNB-CU-UP Software.

## Y.2.2 Threats related to Control plane and User plane in the network

### Y.2.2.1 Control plane data confidentiality protection

- *Threat name*: gNB-CU-UP control plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-CU-UP does not provide confidentiality protection for control plane packets on the E1 reference point, then the control plane packets sent over E1 reference points can be compromised by attackers. This means the UE identifiers, security capabilities, the security algorithms and key materials exchanged can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the E1 reference point is not within the security environment.

- *Threatened Asset*: Mobility Management data.

### Y.2.2.2 Control plane data integrity protection

- *Threat name*: Control plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-CU-UP does not provide integrity protection for control plane packets on E1 reference point, the control plane packets sent over this reference point can be modified without detection. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the E1 reference point are not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data.

### Y.2.2.3 User plane data confidentiality protection

- *Threat name*: User plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-CU-UP does not cipher and decipher user plane packets on the N3/Xn/Uu/F1 reference points, then the attackers can compromise user packets on F1, Uu, Xn-U and N3. The attackers can gain access to user identifiers, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the N3, F1 and Xn reference points are not within the security environment.

- *Threatened Asset*: user plane data.

### Y.2.2.4 User plane data integrity protection

- *Threat name*: User plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-CU-UP does not handle integrity protection for user plane packets for the Xn/N3/Uu/F1 reference points then all the uplink/downlink user plane packets can be manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the Xn, F1 and N3 reference points are not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, User plane data.

**\*\*\*\* NEXT CHANGE \*\*\*\***

Annex Z:   
Aspects specific to the network product class gNB-DU

# Z.1 Network product class description for the gNB-DU

## Z.1.1 Introduction

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

## Z.1.2 Minimum set of functions defining the gNB-DU network product class

As part of the gNB-DU network product, it is expected that the gNB-DU contains gNB-DU application, a set of running processes (typically more than one) executing the software package for the gNB-DU functions and OAM functions that are specific to the gNB-DU network product model. Functionalities specific to the gNB-DU network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.742 [dd].

NOTE: For the purposes of the present document, this common set is defined to be the list of gNB-DU functions contained in 3GPP TS 38.300 [aa], 3GPP TS 38.401 [bb] and TS 23.501 [cc].

# Z.2 Assets and threats specific to the gNB-DU

## Z.2.1 Critical assets

In addition to the critical assets of a GNP described in clause 5.2 of the present document, the critical assets specific to the gNB-DU to be protected are:

- gNB-DU Application;

- Mobility Management data: e.g. QoS and so on, etc;

- User plane data;

- The interfaces of gNB-DU whose data needs to be protected and which are within SCAS scope;

- F1 interface;

- Console interface, for local access: local interface on gNB-DU; and

- OAM interface, for remote access: interface between gNB-DU and OAM system; and

NOTE 1: The detailed interfaces of the gNB-DU class are described in clause 4, Network Product Class Description of the present document.

- gNB-DU Software: binary code or executable code.

NOTE 2: gNB-DU files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, gNB-DU application, Mobility Management data or gNB-DU Software.

## Z.2.2 Threats related to Control plane and User plane in the network

### Z.2.2.1 Control plane data confidentiality protection

- *Threat name*: gNB-DU control plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-DU does not provide confidentiality protection for control plane packets on the F1-C reference point, then the control plane packets sent over F1-C reference point can be compromised by attackers. This means the UE information exchanged can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the F1-C reference points is not within the security environment.

- *Threatened Asset*: Mobility Management data.

### Z.2.2.2 Control plane data integrity protection

- *Threat name*: Control plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-DU does not provide integrity protection for control plane packets on F1-C reference point, the control plane packets sent over this reference point can be modified without detection. The intruder manipulations on control plane packets can lead to denial of service to legitimate users. This threat scenario assumes that the F1-C reference point is not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, Mobility Management data.

### Z.2.2.3 User plane data confidentiality protection

- *Threat name*: User plane data confidentiality protection.

- *Threat Category*: Information Disclosure.

- *Threat Description*: If the gNB-DU does not cipher and decipher user plane packets on the F1 reference point, then the attackers can compromise user packets on F1. The attackers can gain access to user identifiers, serving network identifiers, location information and can perform user tracking. This threat scenario assumes that the F1 reference point are not within the security environment.

- *Threatened Asset*: User plane data.

### Z.2.2.4 User plane data integrity protection

- *Threat name*: User plane data integrity protection.

- *Threat Category*: Tampering data, Denial of Service.

- *Threat Description*: If the gNB-DU does not handle integrity protection for user plane packets for the F1 reference point then all the uplink/downlink user plane packets can be manipulated by intruders to launch Denial of Service attack. This threat scenario assumes that the F1 reference point is not within the security environment.

- *Threatened Asset*: Sufficient Processing Capacity, User plane data.

**\*\*\*\* END OF CHANGES \*\*\*\***