

## Q1: How To Query Encryption and Integrity Switch ?

A: Query by Signal Messages

	Source	Destination	Protocol	TBS for TBI	SQI	Info
22184	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, Registration complete
22184	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, Registration complete
22339	192.168.5.104	192.168.5.27	SJ_NGAP			UplinkNASTransport, Registration complete
14524	192.168.5.104	192.168.5.27	F1AP/SJ_F1AP			MAC=0xf20fdb84
14656	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, UL NAS transport, PDU session establishment request
14656	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, UL NAS transport, PDU session establishment request
15059	192.168.5.104	192.168.5.27	SJ_NGAP			UplinkNASTransport, UL NAS transport, PDU session establishment request
27938	192.168.5.104	192.168.5.27	SJ_NGAP		9	PDU Session Resource Setup Request, DL NAS transport, PDU session establishment accept
29956	192.168.5.104	192.168.5.27	SJ_F1AP			UEContextSetupRequest
35887	192.168.5.104	192.168.5.27	SJ_F1AP			UEContextSetupResponse
38975	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch		9	RRC Reconfiguration, DL NAS transport, PDU session establishment accept
38975	192.168.5.104	192.168.5.27	F1AP/NR RRC			RRC Resume[UNKNOWN PER: too long integer(per_normally_small_nonnegative_whole_number)]
94646	192.168.5.104	192.168.5.27	F1AP/NR RRC			Measurement Report[Malformed Packet]
94646	192.168.5.104	192.168.5.27	SJ_F1AP			RRCDeliveryReport
94763	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch			RRC Reconfiguration Complete
95407	192.168.5.104	192.168.5.27	SJ_F1AP			UEContextModificationRequest

```
> Item 1: id-UL-NGU-UP-TNInformation
> Item 2: id-PDUSessionType
> Item 3: id-SecurityIndication
  > ProtocolIE-Field
    id: id-SecurityIndication (138)
    criticality: reject (0)
    > value
      > SecurityIndication
        integrityProtectionIndication: required (0)
        confidentialityProtectionIndication: required (0)
        maximumIntegrityProtectedDataRate-UL: bitrate64kbs (0)
  > Item 4: id-QoSFlowSetupRequestList
```

5GC: Integrity-ON, Encryption-ON

	Source	Destination	Protocol	TBS for TBI	Redundancy Version for TBI	physCellId	SQI	Info
4:28.522184	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch					UL Information Transfer, Registration complete
4:28.522184	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch					UL Information Transfer, Registration complete
4:28.522339	192.168.5.104	192.168.5.27	SJ_NGAP					UplinkNASTransport, Registration complete
4:31.514524	192.168.5.104	192.168.5.27	F1AP/SJ_F1AP					MAC=0xf20fdb84
4:31.514656	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch					UL Information Transfer, UL NAS transport, PDU
4:31.514656	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch					UL Information Transfer, UL NAS transport, PDU
4:31.515059	192.168.5.104	192.168.5.27	SJ_NGAP					UplinkNASTransport, UL NAS transport, PDU sess
4:31.527938	192.168.5.104	192.168.5.27	SJ_NGAP				9	PDU Session Resource Setup Request, DL NAS transpo
4:31.529956	192.168.5.104	192.168.5.27	SJ_F1AP					UEContextSetupRequest
4:31.535887	192.168.5.104	192.168.5.27	SJ_F1AP					UEContextSetupResponse
4:31.538975	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch				9	RRC Reconfiguration, DL NAS transport, PDU ses
4:31.538975	192.168.5.104	192.168.5.27	F1AP/NR RRC					RRC Resume[UNKNOWN PER: too long integer(per_n
4:31.594646	192.168.5.104	192.168.5.27	F1AP/NR RRC					Measurement Report[Malformed Packet]
4:31.594646	192.168.5.104	192.168.5.27	SJ_F1AP					RRCDeliveryReport
4:31.594763	192.168.5.104	192.168.5.27	SJ_NrRrcUIdcch					RRC Reconfiguration Complete
4:31.595407	192.168.5.104	192.168.5.27	SJ_F1AP					UEContextModificationRequest

```
> pdcp-Config
  > drb
    discardTimer: ms1500 (14)
    pdcp-SN-SizeUL: len18bits (1)
    pdcp-SN-SizeDL: len18bits (1)
    > headerCompression: notUsed (0)
      notUsed: NULL
    statusReportRequired: true (0)
    t-Reordering: ms120 (15)
    cipheringDisabled: true (0)
  > measConfig
    > measObjectToAddModList: 1 item
      > Item 0
```

gNB: Integrity-Off, Encryption-Off

	Destination	Protocol	TBS for TBI	Redundancy Version for TBI	physCellId	SQI	Info
104	192.168.5.27	SJ_NrRrcUIdcch					UL Information Transfer, UL NAS transport, PDU session establishment
104	192.168.5.27	SJ_NGAP					UplinkNASTransport, UL NAS transport, PDU session establishment requ
104	192.168.5.27	SJ_NGAP				9	PDU Session Resource Setup Request, DL NAS transport, PDU session establi
104	192.168.5.27	SJ_F1AP					UEContextSetupRequest
104	192.168.5.27	SJ_F1AP					UEContextSetupResponse
104	192.168.5.27	SJ_NrRrcUIdcch				9	RRC Reconfiguration, DL NAS transport, PDU session establishment acc
104	192.168.5.27	F1AP/SJ_F1AP					MAC=0x1078a7e5
104	192.168.5.27	F1AP/SJ_F1AP					MAC=0xb7adb528
104	192.168.5.27	SJ_F1AP					RRCDeliveryReport
104	192.168.5.27	SJ_NrRrcUIdcch					RRC Reconfiguration Complete
104	192.168.5.27	SJ_F1AP					UEContextModificationRequest
104	192.168.5.27	SJ_F1AP					UEContextModificationResponse
104	192.168.5.27	SJ_NGAP					PDU Session Resource Setup Response

```
> mappedQoS-FlowsToAdd: 1 item
  > Item 0
    QFI: 1
  > drb-Identity: 1
  > pdcp-Config
    > drb
      discardTimer: ms1500 (14)
      pdcp-SN-SizeUL: len18bits (1)
      pdcp-SN-SizeDL: len18bits (1)
      > headerCompression: notUsed (0)
        notUsed: NULL
      integrityProtection: enabled (0)
      statusReportRequired: true (0)
      t-Reordering: ms120 (15)
  > measConfig
```

gNB: Integrity-ON, Encryption-ON

n	Protocol	TBS for TBI	Redundancy Version for TBI	physCellId	SQI	Info
15.27	SJ_NGAP					InitialContextSetupResponse
15.27	SJ_NrRrcUIdcch					UL Information Transfer, Registration complete
15.27	SJ_NrRrcUIdcch					UL Information Transfer, Registration complete
15.27	SJ_NGAP					UplinkNASTransport, Registration complete
15.27	F1AP/SJ_F1AP					UL Information Transfer MRDC MAC=0x98ade0b9
15.27	SJ_NrRrcUIdcch					UL Information Transfer, UL NAS transport, PDU session establishment request
15.27	SJ_NrRrcUIdcch					UL Information Transfer, UL NAS transport, PDU session establishment request
15.27	SJ_NGAP					UplinkNASTransport, UL NAS transport, PDU session establishment request
15.27	SJ_NGAP					9 PDU Session Resource Setup Request, DL NAS transport, PDU session establishment accept
15.27	SJ_F1AP					UEContextSetupRequest
15.27	SJ_F1AP					UEContextSetupResponse
15.27	SJ_NrRrcUIdcch					9 RRC Reconfiguration, DL NAS transport, PDU session establishment accept
15.27	F1AP/SJ_F1AP					MAC=0x7dd420737
15.27	F1AP/SJ_F1AP					UL Dedicated MessageSegment MAC=0x8eb49126
15.27	SJ_F1AP					RRCDeliveryReport
15.27	SJ_NrRrcUIdcch					RRC Reconfiguration Complete

```

drb-Identity: 1
  pdcp-Config
    drb
      discardTimer: ms1500 (14)
      pdcp-SN-SizeUL: len18bits (1)
      pdcp-SN-SizeDL: len18bits (1)
      headerCompression: notUsed (0)
      notUsed: NULL
      statusReportRequired: true (0)
      t-Reordering: ms120 (15)

```

gNB: Integrity-Off, Encryption-On

No	Time	Source	Destination	Protocol	TBS for TBI	SQI	Info
2023-06-01	16:07:55.095715	192.168.5.115	192.168.5.27	SJ_F1AP			RRCDeliveryReport
2023-06-01	16:07:55.095715	192.168.5.115	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, Security mode complete, Re
2023-06-01	16:07:55.095715	192.168.5.115	192.168.5.27	SJ_NrRrcUIdcch			UL Information Transfer, Security mode complete, Re
2023-06-01	16:07:55.096124	192.168.5.115	192.168.5.27	SJ_NGAP			UplinkNASTransport, Security mode complete, Registr
2023-06-01	16:07:55.103274	192.168.5.115	192.168.5.27	SJ_NGAP			InitialContextSetupRequest, Registration accept
2023-06-01	16:07:55.104730	192.168.5.115	192.168.5.27	SJ_NrRrcUIdcch			Security Mode Command
2023-06-01	16:07:55.104730	192.168.5.115	192.168.5.27	F1AP/SJ_F1AP			Security Mode Command MAC=0xcd38ce15
2023-06-01	16:07:55.125379	192.168.5.115	192.168.5.27	F1AP/SJ_F1AP			Security Mode Complete MAC=0x15dd0bc1
2023-06-01	16:07:55.125717	192.168.5.115	192.168.5.27	SJ_F1AP			RRCDeliveryReport
2023-06-01	16:07:55.125717	192.168.5.115	192.168.5.27	SJ_NrRrcUIdcch			Security Mode Complete
2023-06-01	16:07:55.126923	192.168.5.115	192.168.5.27	SJ_NrRrcUIdcch			UE Capability Enquiry

> Frame 3329: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF\_{97D682D3-F0B3-4822-96FE-C9B34542C5DA}, id 0  
 > Ethernet II, Src: AdlinkTe\_6e:65:00 (00:30:64:6e:65:00), Dst: 98:8f:e0:66:b5:1e (98:8f:e0:66:b5:1e)  
 > Internet Protocol Version 4, Src: 192.168.5.115, Dst: 192.168.5.27  
 > User Datagram Protocol, Src Port: 57583, Dst Port: 50154  
 > CpCellApp

```

NR Radio Resource Control (RRC) protocol
  DL-DCCH-Message
    message: c1 (0)
      c1: securityModeCommand (4)
        securityModeCommand
          rrc-TransactionIdentifier: 0
          criticalExtensions: securityModeCommand (0)
            securityModeCommand
              securityConfigSMC
                securityAlgorithmConfig
                  cipheringAlgorithm: nea0 (0)
                  integrityProtAlgorithm: nia2 (2)

```

Algorithm for Encryption and Integrity

## Q2: How Turn off Encryption and Integrity Switch ?

A: Turn on and off by odi commands

- ① odi -n cpcellapp0 fto-set-security-mod-enable 1703939 1
- ② odi -n cpcellapp0 fto-set-integrity-ue-enable 1703939 0
- ③ odi -n cpcellapp0 fto-set-cipher-ue-enable 1703939 0

Note: cpcellapp0 indicates Cell ID 1, 1703939 indicates NRCCellID, 1 indicates switch turns on, 0 indicates switch turns off.

Commands Combination For Different Function:

- ①1-②0: Indicates Integrity off, encryption off.
- ①1-②0-③0: Indicates Integrity off, encryption off.
- ①1-②1-③0: Indicates Integrity on, encryption off.
- ①1-②0-③1: Indicates Integrity off, encryption on.