

# Consideration of CPSR message encoding with EDT in 5GCN

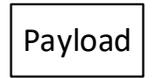
Vodafone

# Why would someone develop 5GC for NB-IoT?

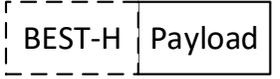
We need compelling reason – Maximize Battery Life by sending NB-IoT data via Early-Data-Transmission (EDT).

**This proposal cuts TBS size by 35% (63 vs 41) compared to EPC. Therefore genuine, real life battery life improvement.**

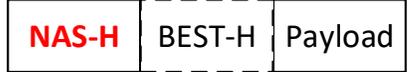
# Structure of NB-IoT data including headers



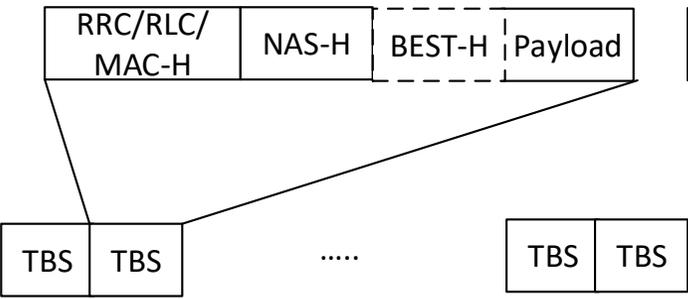
Useful payload size: 30 bytes  
 1 byte length indicator  
 64 bit source ID;  
 64 bit destination ID;  
 32 bit timestamp (one second granularity over 100 years)  
 16 bit data type identifier (e.g. temperature vs location vs humidity)  
 16 bit data value (e.g. temperature)  
 5 byte UE-enterprise integrity check (MAC+SN)



BEST-H (UE to enterprise MAC-I TS33.163): 9 bytes  
 1 bit UP/CP flag  
 1 bit RFU  
 3 bit key ID  
 11 bit UP COUNTER  
 1 byte Session ID  
 2 byte Data length  
 4 byte MAC



**NAS-H = n bytes (tbd)**



RRC/RLC/MAC-H = 8-9 bytes for EDT on uplink CCCH including 48 bits 5G-S-TMSI

# BEST: user plane type 01 message contents

User Plane type 01 message:								
UP / CP Flag	RFU	Key ID	UP COUNTER	Session ID	Data Length	Data	MAC	
1 bit	1 bit	3 bits	Note 4	Note 1 Note 2	Note 1 Note 2 Note 3	Note 2 Note 3	Note 1 Note 3	

1 bit UP/CP flag

1 bit Reserved for Future Use (RFU)

3 bit key ID

11 bit User Plane (UP) COUNTER

1 byte Session ID

2 byte Data length

4 byte Message Authentication Code (MAC)

\* BEST: Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST) in 3GPP TS33.163

# 3GPP TS 36.331 – TBS for NB-IoT EDT

```
EDT-TBS-NB-r15 ::= SEQUENCE {  
    edt-SmallTBS-Enabled-r15    BOOLEAN,  
    edt-TBS-r15                 ENUMERATED {b328, b408, b504, b584, b680, b808, b936, b1000}
```

They are 41 bytes, 51 bytes, 63 bytes, 73 bytes, 85 bytes, 101 bytes, 117 bytes, 125 bytes.

# Summary

- *When using BEST, it is possible to remove the 5 byte UE-enterprise integrity check of the Payload. Additionally, if we reduce the 64 bit source and destination IDs from 64 bit to 32 bit, the length of Payload is then 16 bytes. This leads to the size of the layer 1 data unit to be Payload + BEST header + NAS header (n) + RRC/RLC/MAC header = 17+9+n+9 = 35+n, where n is the length of the CPSR message header to be specified.*
- *This means that in order to match the minimum TBS size of 41 bytes used by NB-IoT EDT, the maximum length of the NAS CPSR message header amounts to **6 bytes**.*
- *IoT is kind of “permanent roaming” business in which the HPLMN cannot make proper assumptions about the VPLMN. Therefore, the HPLMN needs to optimize the IoT applications to the EDT payload that is likely to be available with the biggest geographic spread. This payload will be the smallest value of 41 bytes.*
- *Another use case is that when BEST is not used (disadvantageous security protection of non-ip data), we end up with Payload + NAS header (n) + RRC/RLC/MAC header = 22+n+9 = 31+n, the maximum length of the NAS CPSR message header amounts to **10 bytes**.*

# Rel-15 5GC NAS message (security protected) format

8	7	6	5	4	3	2	1	
Extended protocol discriminator								octet 1
Security header type associated with a spare half octet								octet 2
								octet 3
Message authentication code								
								octet 6
Sequence number								octet 7
								octet 8
Plain 5GS NAS message								
								octet n

Total size of message header: 10 octets plus SM message header

Extended protocol discriminator	octet 1
Security header type associated with a spare half octet; or PDU session identity	octet 2
Message type	octet 3
	octet 4
Other information elements as required	
	octet n

# CPSR Coding Considerations (1)

- Introduce a new EPD value set to control plane CloT Data and the message is integrity protected and ciphered. This enables to remove the “Security header type”, “Spare half octet” and “Control plane service request message identity”

Result: Reduce 2 octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 A new EPD set to Control Plane CloT Data. This means also that the security header type is “Integrity protected and ciphered NAS message” (see clause 9.3 of TS 24.301)	M	V	1
-	<del>Security header type</del>	<del>Security header type 9.3</del>	<del>M</del>	<del>V</del>	<del>1/2</del>
-	<del>Spare half octet</del>	<del>Spare half octet 9.5</del>	<del>M</del>	<del>V</del>	<del>1/2</del>
-	<del>Control plane service request message identity</del>	<del>Message type 9.7</del>	<del>M</del>	<del>V</del>	<del>1</del>
	ngKSI	NAS key set identifier 9.11.3.32	M	V	1/2
	Control plane service type	Control plane service type 9.11.3.a	M	V	1/2

# Initial UE message

IE/Group Name	Presence	Range	IE type and reference	Semantics description	Criticality	Assigned Criticality
Message Type	M		9.3.1.1		YES	ignore
RAN UE NGAP ID	M		9.3.3.2		YES	reject
NAS-PDU	M		9.3.3.4		YES	reject
User Location Information	M		9.3.1.16		YES	reject
RRC Establishment Cause	M		9.3.1.111		YES	ignore
5G-S-TMSI	O		9.3.3.20		YES	reject
AMF Set ID	O		9.3.3.12		YES	ignore
UE Context Request	O		ENUMERATED (requested, ...)	Indicates that a UE context including security information needs to be setup at the NG-RAN.	YES	ignore
Allowed NSSAI	O		9.3.1.31		YES	reject

3GPP TS 38.413

AMF will not process just NAS-PDU without also using the other N2AP IEs

3GPP TS 38.413

# CPSR Coding Considerations (2)

- The “Control plane service type” (MO or MT) is included in the RRC establishment cause and the NGAP Initial UE message. Similar to the 5G-S-TMSI, the AMF can obtain this information about Control plane service type from lower layers.

Result: Reduce 1/2 octet

- Importantly, the AMF can also get the length of the NAS PDU included in the Initial UE message. Thus, the CloT Data Container IE can coded as V-format. **This saves up to 4 Octets.**

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 A new EPD set to Control Plane CloT Data. This means also that the security header type is “Integrity protected and ciphered NAS message” (see clause 9.3 of TS 24.301)	M	V	1
-	<del>Security header type</del>	<del>Security header type 9.3</del>	<del>M</del>	<del>V</del>	<del>1/2</del>
-	<del>Spare half octet</del>	<del>Spare half octet 9.5</del>	<del>M</del>	<del>V</del>	<del>1/2</del>
-	<del>Control plane service request message identity</del>	<del>Message type 9.7</del>	<del>M</del>	<del>V</del>	<del>1</del>
	ngKSI	NAS key set identifier 9.11.3.32	M	V	1/2
-	<del>Control plane service type</del>	<del>Control plane service type 9.11.3.a</del>	<del>M</del>	<del>V</del>	<del>1/2</del>
	CloT Data Container	CloT Data Container	M	V	3-n

# CPSR Coding Considerations (3)

- *TS33.501 6.2.3.2 Key identification*

The key KAMF shall be identified by the key set identifier ngKSI. ngKSI may be either of type native or of type mapped. An ngKSI shall be stored in the UE and the AMF together with KAMF and the temporary identifier 5G-GUTI, if available.

- As Contexts in the UE and the AMF are perfectly synced when the UE sending the CPSR (unlike sending the REGISTRATION REQUEST message), the AMF can retrieve the ngKSI and KAMF from the 5G-GUTI.

Result: Reduce 1/2 octet

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 A new EPD set to Control Plane CloT Data. This means also that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301)	M	V	1
-	Security header type	Security header type 9.3	M	∅	1/2
-	Spare half octet	Spare half octet 9.5	M	∅	1/2
-	Control plane service request message identity	Message type 9.7	M	∅	1
-	ngKSI	NAS key set identifier 9.11.3.32	M	∅	1/2
-	Control plane service type	Control plane service type 9.11.3.a	M	∅	1/2
	CloT Data Container	CloT Data Container	M	V	3-n

# CPSR Coding Considerations (4)

- Using a short MAC-I

**Result: Reduce 2 octet**

## NOTE:

1. Enterprises need to use end to end integrity protection (or “BEST end to HPLMN” plus “IPSec HPLMN to Enterprise” integrity protection). Hence there is no great benefit in the VPLMN providing UE to AMF data integrity protection. However, some protection mechanism is needed to stop criminals hijacking the VPLMN’s radio link and sending data that accumulates charges on someone else’s bill. A short 2 bytes MAC-I is sufficient for that task.
2. Short MAC-I has been used for Service Request message (32 bits) in EPC.

# Summary

- This leads us to have a 4-Octet-header for 5GC control plane CloT data message. This format can also be used for the UE sending subsequent CloT data.

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number	M	V	1

# CPSR message coding (Alt-1): header = 5 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CIoT Data Container	CIoT Data Container	M	V	1-n

Integrity Protected

Ciphered

PDU session identity	DDX	Data type	octet 1
CIoT data container value			octet 2-n

NOTE:

1. CIoT data container IE is mandatory, and the length of the NAS PDU including small data can be obtained from the lower layers. Extension of the outer header by adding more IEs in the future can be achieved by keeping a reserved value within the Data Type field or using 3 bit PDU Session ID, or by using another EPD value.
2. When Slicing is used, both AMF and SMF can be optimized for CIoT data traffic.

# Consideration of different use cases

IEI	Information Element	Type/Reference	Presence	Format	Length				
	Extended protocol discriminator	Extended protocol discriminator	M	V	1				
	Message authentication code	Short MAC-I	M	V	2				
	Sequence number	Sequence number	M	V	1				
	CIoT Data Container	CIoT Data Container	C	V	0-n				

PDU session identity	DDX	Data type	octet 1
CIoT data container value			octet 2-n

- Uplink

1. The same message can be used for the subsequent data to be sent

The AMF detect the differences between Idle mode CPSR and Connected Mode Subsequent Data/CPSR from the use of N2-AP Initial UE Message vs N2-AP Uplink NAS Transport. For the Initial UE Message, the AMF performs the other necessary checks (e.g. that the N2-AP Location Information shows that the UE is allowed to do this action in this geographic area).

2. The same message can be used for the UE in 5GMM-CONNECTED mode CPSR.

The AMF can keep track of which PDU sessions have been „activated“ and when the AMF receives a data packet with a non-activated PDU identity, the AMF can e.g. use the N2-AP location information to check that this PDU session is permitted in this location (etc)

3. The message without including „CIoT Data Container“ can be used as paging response.

The length of the N2-AP NAS PDU is then 4 octets and there is no CIoT Data Container.

- Downlink (DDX is not used)

1. The same message can be used to send the DL 5GMM message (e.g. Service Accept message).

2. The same message can be used to send the MT CP CIoT data.

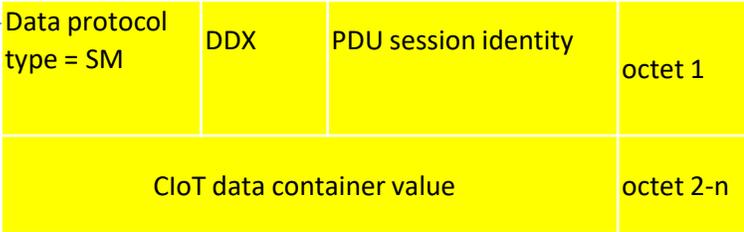
# CPSR message coding (Alt-1a): header = 5 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request. This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CloT Data Container	CloT Data Container	M	V	0-n

**data protocol = SM data**

**Integrity Protected**

**Ciphered**



NOTE: Data Protocol Type field indicates SM data (for sending MO CP CloT data)

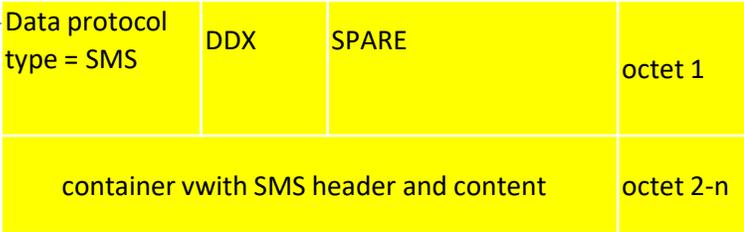
# CPSR message coding (Alt-1b): header = 5 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CloT Data Container	CloT Data Container	M	V	0-n

data protocol = SMS

Integrity Protected

Ciphered



NOTE: Data Protocol Type field indicates SMS (for sending MO SMS)

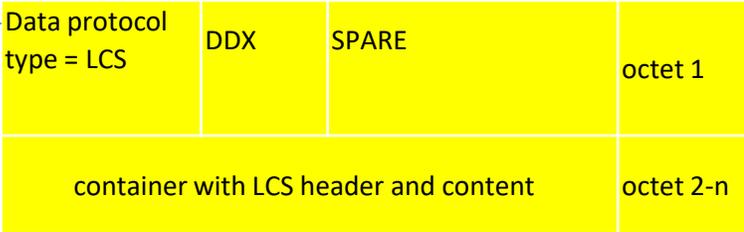
# CPSR message coding (Alt-1c): header = 5 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request. This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CloT Data Container	CloT Data Container	M	V	0-n

data protocol = LCS

Integrity Protected

Ciphered



NOTE: Data Protocol Type field indicates LCS data (for sending LCS data)

# Paging response CPSR message coding (Alt-1x): header = 4 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1

NOTE: If the AMF has sent N2 paging , then ANY (and every) establishment of N2 connection for that UE shall be regarded as a Paging Response.

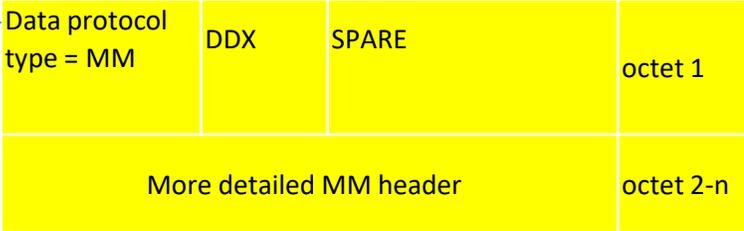
# CPSR message coding (Alt-1y): Complex MM function

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request. This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CIoT Data Container	CIoT Data Container	M	V	0-n

**data protocol = MM**

**Integrity Protected**

**Ciphered**



NOTE: Data Protocol Type field indicates MM (for sending DL MM Message)

# CPSR message coding (Alt-2): header = 6 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CIoT Data Container	CIoT Data Container	M	LV	1-n

Integrity Protected

Ciphered

Length of CIoT data container			octet 1
PDU session identity	DDX	Data type	octet 2
CIoT data container value			octet 3-n

NOTE: CIoT data container IE is mandatory, and with a length indicator that enables future extensions of adding more IEs.

# CPSR message coding (Alt-3): header = 7 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CIoT Data Container	CIoT Data Container	O	TLV	1-n

Integrity Protected

Ciphered

IEI			octet 1
Length of CIoT data container			octet 2
PDU session identity	DDX	Data type	octet 3
CIoT data container value			octet 4-n

NOTE: In order to allow sending CPSR w/o the CIoT data container IE, the CIoT data container IE is optional with a length indicator of 1 octet (Small data).

# CPSR message coding (Alt-3 cont.): header = 8 Octets

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2 set to Control Plane Service Request.  This means that the security header type is "Integrity protected and ciphered NAS message" (see clause 9.3 of TS 24.301).	M	V	1
	Message authentication code	Short MAC-I	M	V	2
	Sequence number	Sequence number 9.10	M	V	1
	CIoT Data Container	CIoT Data Container	O	TLV-E	1-n

Integrity Protected

Ciphered

IEI			octet 1
Length of ClIoT data container			octet 2-3
PDU session identity	DDX	Data type	octet 4
ClIoT data container value			octet 5-n

NOTE: In order to allow sending CPSR w/o the ClIoT data container IE, the ClIoT data container IE is optional with a length indicator of 2 octets (Large data).

# Conclusion

- The CPRS in EPC with RAI has 18 Octets header size, whereas the Alt-1 of CPRS in 5GC with RAI has now 5 Octets.

It gives rise to a 72% (18 vs 5) saving of the NAS message header size.

**When considering the TBS size to be used, it is 35% (63 vs 41) saving compared to EPC.**



This evident improvement compared to the 4G-CIoT mobile system will motivate the network operators and network vendors to build up the CloT economic system with 5GCN.

With the further optimization in CT1#119, it is 58% (12 vs 5) for header and 20% (51 vs 41) for TBS.

# Appendix (1): Additional considerations

- In CT1 CC on August 1st, an additional 70 bytes IP type of payload was raised and discussed. When a fully optimised non-IP Type PDN connection is used for the NB-IoT data transmission, the useful data in the payload will then be  $70-28=42$  bytes (IPv4) and  $70-48=22$  bytes (IPv6). This number is pretty much inline with the payload size used in this discussion paper.

# Appendix (2): UL NAS TRANSPORT message

IE/Group Name	Presence	Range	IE type and reference	Semantics description	Criticality	Assigned Criticality
Message Type	M		9.3.1.1		YES	ignore
AMF UE NGAP ID	M		9.3.3.1		YES	reject
RAN UE NGAP ID	M		9.3.3.2		YES	reject
NAS-PDU	M		9.3.3.4		YES	reject
User Location Information	M		9.3.1.16		YES	ignore

3GPP TS 38.413

# Appendix (3): New EPD

## TS 24.007 Table 11.2.3.1.1A.1: EPD values

EPD value (octet 1, bit 1 to bit 8)								
Bits								
8	7	6	5	4	3	2	1	
0	0	0	0	1	1	1	0	reserved
0	0	0	1	1	1	1	0	reserved
0	0	1	0	1	1	1	0	5GS session management messages
0	0	1	1	1	1	1	0	reserved
0	1	0	0	1	1	1	0	reserved
0	1	0	1	1	1	1	0	reserved
0	1	1	0	1	1	1	0	reserved
0	1	1	1	1	1	1	0	5GS mobility management messages
1	0	0	0	1	1	1	0	reserved
1	0	0	1	1	1	1	0	reserved
1	0	1	0	1	1	1	0	reserved
1	0	1	1	1	1	1	0	reserved
1	1	0	0	1	1	1	0	5GS Control Plane Clot data message reserved
1	1	0	1	1	1	1	0	reserved
1	1	1	0	1	1	1	0	reserved
1	1	1	1	1	1	1	0	reserved

NOTE: Bits 4 to 1 of each EPD value contain "extension of the PD to one octet length" as specified in subclause 11.2.3.1.1.