**3GPP TSG-CT WG1 Meeting #125-eC1-204552**

**Electronic meeting, 20-28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **27.007** | **CR** | **0699** | **rev** | **-** | **Current version:** | **16.5.0** |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | AT command for NAS messages between MT and TE |
|  |  |
| ***Source to WG:*** | OPPO |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | Vertical\_LAN |  | ***Date:*** | 2020-08-13 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-16 |
|  | *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 canbe 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | As discussed in C1-204551, for access to PLMN services via SNPN (or access to SNPN services via PLMN) the NAS signalling procedures sends and receives NAS signalling messages from the AMF in the PLMN (or in the SNPN) not through an RRC connection but instead over the data radio bearers of a PDU Session – in short this is NAS signalling over PDU Session instead of over a RRC connection.For a UE configuration where the NAS stack and machine are in the Mobile Terminal (MT) while application layers that manages the PDU Sessions are in the Terminal Equipment (TE), an AT CMD command and an unsolicited report are proposed here to transfer the peer-to-peer NAS signalling messages from MT to TE and a new unsolicited report AT CMD for the NAS messages to go from TE to MT.. |
|  |  |
| ***Summary of change:*** | The AT CMD +CNASMSGC and +CNSGMSGR are introduced. |
|  |  |
| ***Consequences if not approved:*** | UE configurations where the NAS is on the MT while the application layers are on the TE, will not be able to support NAS over PDU and so not be able to support access to PLMN services via SNPN (or access to SNPN services via PLMN) |
|  |  |
| ***Clauses affected:*** | 8.83 (new), 8.84 (new), 8.85 |
|  |  |
|  | **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:*** |  |

\* \* \* First Change \* \* \* \*

## 8.83 Application level NAS message command +CNASMSGC

Table 8.83-1: +CNASMSGC action command syntax

|  |  |
| --- | --- |
| Command | Possible response(s) |
| +CNASMSGC=<upp\_layer\_msg\_length>,<upp\_layer-nas-msg> | *+CME ERROR: <err>* |
| +CNASMSGC=? |  |

**Description**

According to 3GPP TS 23.501 [165], the access to PLMN services via SNPN (or the access to SNPN services via PLMN), relies on the UE's NAS able to interact with the NAS of the PLMN (or the SNPN) not over a RRC connection but over an EAP-5G signaling control layer placed over the PDU layer (in 3GPP TS 23.501 [165] terminology). This means that the peer-to-peer NAS signalling messages are transferred between UE and PLMN (or SNPN) over the data radio bearers of a PDU Session of the PDU layer and then over the network user plane functions of the underlying SNPN (or PLMN).

With the MT – TE separation where the NAS state machines are in the MT while the applications managing and controlling the PDU layer are in the TE – along with the EAP-5G being in the TE – there is a need to transfer the NAS signalling messages between the MT and the TE.

This command +CNASMSGC allows NAS (at a protocol layer below the applications) in the MT to provide to the application layer (the upper layers in the TE), a NAS signalling message as defined in 3GPP TS 24.501 [161]. Refer subclause 9.2 for possible <err> values.

**Defined values**

<cid>: integer type: specifies a particular QoS flow definition.

<upp\_layer\_msg\_length>: integer type. Indicates the number of octets of the <upp\_layer-nas-msg> parameter.

<upp\_layer-nas-msg>: string of octets. Contains the NAS signalling message to be transferred, or that was received, over data bearers.

**Implementation**

Optional.

\* \* \* Next Change \* \* \* \*

## 8.84 Application level NAS message report +CNASMSGR

Table 8.84-1: +CNASMSGR action command syntax

|  |  |
| --- | --- |
| Command | Possible response(s) |
| +CNASMSGR=<upp\_layer\_msg\_length>,<upp\_layer-nas-msg> | *+CME ERROR: <err>* |
| +CNASMSGR=? |  |

**Description**

According to 3GPP TS 23.501 [165], the access to PLMN services via SNPN (or the access to SNPN services via PLMN), relies on the UE's NAS able to interact with the NAS of the PLMN (or the SNPN) not over a RRC connection but over an EAP-5G signaling control layer placed over the PDU layer (in 3GPP TS 23.501 [165] terminology). This means that the peer-to-peer NAS signalling messages are transferred between UE and PLMN (or SNPN) over the data radio bearers of a PDU Session of the PDU layer and then over the network user plane functions of the underlying SNPN (or PLMN).

With the MT – TE separation where the NAS state machines are in the MT while the applications managing and controlling the PDU layer are in the TE – along with the EAP-5G being in the TE – there is a need to transfer the NAS signalling messages between the MT and the TE.

This command +CNASMSGR allows the application layer (the upper layers in the TE) to provide to the NAS (at a protocol layer below the applications ) in the MT, an unsolicited report containing the NAS signalling message received over the data radio bearer of the PDU Session. Refer subclause 9.2 for possible <err> values.

**Defined values**

<cid>: integer type: specifies a particular QoS flow definition.

<upp\_layer\_msg\_length>: integer type. Indicates the number of octets of the <upp\_layer-nas-msg> parameter.

<upp\_layer-nas-msg>: string of octets. Contains the NAS signalling message to be transferred, or that was received, over data bearers.

**Implementation**

Optional.

\* \* \* Next Change \* \* \* \*

## 8.85 Informative examples

Phone Activity Status (+CPAS) is a general command used to detect the presence of the MT, if there is an incoming call, or if there is a call in progress. This command is normally used before trying to operate the MT from the TE. Note that the activity status can change at any time after the execution of +CPAS, and hence the returned value can be obsolete. Detachment of the MT from the TA is indicated with a special final result code that indicates all errors related to the operation of the MT. Result code is +CME ERROR: <err>, where <err> is an integer or verbose value giving useful information about the reason for the command failure (refer subclause "Mobile termination error result code +CME ERROR").

Set Phone Functionality (+CFUN) can be used to reset the MT or set the power consumption level of the MT by disabling certain parts of the MT (e.g. the transmit and receive RF circuits). Mobile Termination Control Mode (+CMEC) is a command which manages access sharing between the MT and the TE to operate the user interface of the MT. It has four subparameters which describe the access to keypad, display, indicators, and touch screen. Each subparameter has values for restricting the operation of the corresponding user interface part only to the MT or only to the TE, or to give the access for both of them.

Keypad Control command (+CKPD) is used to operate the keypad of the MT. Here lies the problem of different keypad types between manufacturers, and also between their MT models. The keypresses are sent to the MT as a string type subparameter of this command. Each character in that string represents a key which will be logically pressed. A special character (colon) followed by any character can be used by manufacturers (or TE application programmers) to represent a key which is not defined in this profile. An escape character (semicolon) for direct string entering is also defined. All text between single semicolon characters is treated as an alphanumeric entry and is not converted to keypressings. All semicolon characters inside the text is duplicated in the TE and stripped back to one before entering them to the MT. Command has also optional second and third parameters which can be used to alter the time to strike each key, and the pause to wait between keystrokes (in tenths of a second). A special pause character (W or w) can be added in the string type subparameter for an extra pause of the same length as given by the third subparameter. In the following example alphanumeric mode is entered and a person predefined in the MT phonebook, "Ilkka", is called; each key is struck for half a second and pauses between strokes are a tenth of a second:

AT+CKPD="@:Ilkka:S",5,1

OK

Display Control command (+CDIS) is used both for writing to the display text fields and for reading the current status of the fields. Mobile Termination usually has a character set of its own, so the TA will do a conversion between the TE and the MT character sets. TE can have several character sets and the TA must be informed of the character set in use before starting to write or read the display. Character set is set with general command select TE character set +CSCS. The +CDIS=? query command is a way to get information about the length of the fields. In the following example an MT is first queried about the supported conversions and the lengths of the fields. The response shows there are three ten character long and two six character long fields. Then the TE character set is set to be IRA and the current status of the display is read. The last command writes the text "Hello, I'm writing to display" in the three fields, and keeps the contents of the two other fields same (the last two commas could also be left out).

AT+CSCS=?;+CDIS=?

+CSCS: ("IRA","PCCP850","8859‑1")

+CDIS: 10,10,10,6,6

OK

AT+CSCS="IRA"

OK

AT+CDIS?

+CDIS: "RADIOLINJA","","","Menu","Memory"

OK

AT+CDIS="IRA","Hello, I'm","writing to","display",,

OK

The writing is possible only when it is permitted by the Mobile Termination Control Mode command (and by the manufacturer). If a certain field is not writable (but is readable), writing to it is ignored. The order of the text fields is determined by manufacturers and follow the rule: first field is in the upper left corner, second in the next field to the right, and so on, until to the last field in the lower right corner.

Touch screen action Control command (+CTSA) is used to operate the touch screen of the MT. The x, y coordinates of the phone are fixed even if the device's orientation is changed. In the following example commands are sent to the MT to emulate a user drawing on the ME's touch screen; it is relevant that the gesture starts from the top of the touch screen. A gesture is emulated, starting at location 10,10 in a non-display area of the ME’s (touch) screen, then dragged to 50,50 (during which the gesture crosses the boundary between the non-display area and a display area), then dragged to 100,100 and finally the touch screen is released at location 100,100.

AT+CSO=? obtain the touch screen orientation

+CSO=2,0

AT+CSS=? obtain the touch screen size
+CSS=200,600
AT+CDSB=? determine if a boundary between the non-display area and a display area exists, and its location
+CDSB=20,20,180,580
AT+CTSA=1,10,10 start emulating a gesture
AT+CTSA=1,50,50 emulate that the gesture crosses the boundary between non-display area and a display area
+CTSA=0,100,100 end emulating the gesture

Indicators can be handled with Indicator Control command (+CIND). Its query command returns a short description (abbreviation) of the purpose of the indicators and the supported values for each indicator. The setting and reading is done similarly as with Display Control command. In the following example the indicators of a phone are queried, their current value is read, and the value of message indicator is tried to set (but it is forbidden):

AT+CIND=?

+CIND: ("memory",(0‑2)),("call",(0,1)),("data",(0,1)),("roam",(0,1)),

("alpha",(0,1)),("message",(0,1)),("index1",(0‑11)),("index2",(0‑11)),

("index3",(0‑11)),("signal",(0‑5)),("service",(0,1)),("sel1",(0,1)),

("sel2",(0,1)),("sel3",(0,1)),("battchg",(0‑5))

OK

AT+CIND?

+CIND: 1,0,0,0,0,1,0,0,0,3,1,0,0,0,5

OK

AT+CIND=,,,,,0

+CME ERROR: 10

The subparameter order in the command is defined by the query command order, not by the actual display order. The zero value of an indicator means that it is off (or in state which can be identified as "off"‑state), value one means that the indicator is on (or in a state which is more substantial than "off"‑state), value two is more substantial than one, and so on.

To this point, only operating through the TE is covered. But when MT can be operated also through its keypad, or touch screen, or there are changes in the status of the display elements, the information about these actions is given to the TE also. This can be solved only with unsolicited result codes which return keypad, display text and indicator, and touch screen events. Each event group has a result code of its own: +CKEV returns the key code and if the key pressed (1) or released (0), +CDEV returns the display text field running number (as specified by command +CDIS) and the new status of the field, and +CIEV returns the running number of the indicator (refer +CIND) and the new value of it, and +CTEV returns the location of the action performed on the touch screen. In the following example number key 1 is pressed, updated on the display, released, and signal strength changes its state to five, the touch screen is pressed at coordinates 10,10, and it is released at the same coordinates, 3 seconds after initially pressing the screen:

+CKEV: 49,1

+CDEV: 1,"1"

+CKEV: 49,0

+CIND: 10,5

+CTEV: 1,10,10,0;

+CTEV: 0,10,10,0,3000

Mobile Termination Event Reporting command (+CMER) has been specified for the purpose of controlling the sending of these unsolicited result codes to the TE. Four ways are provided to handle the buffering of the result codes (see figure 8). The first is to buffer them always. The second possibility is to discard them when in on‑line data mode and otherwise forward them directly to the TE. The third possibility is to buffer them in data mode and otherwise forward them to the TE. The last possibility is to send them always to the TE (some inband technique - e.g. V.80 - is used in data mode to send the result codes within the data). This is the first subparameter of +CMER command. Next three subparameters are used to enable or disable each of the keypad, text field and indicator result codes. Sending codes can be enabled either so that only events generated from the MT user interface are returned, or so that also events caused by Keypad, Display and Indicator Control commands are returned. The fifth subparameter controls the flushing of the buffer when the value of the first subparameter is changed to a value from one to three.



Figure 8: Mobile termination event reporting

An example of complete setup of the TA where TE takes the control of keypad, but does not want to write to display nor control the indicators (in the start MT is powered off):

AT+CMEE=2;+CREG=1 (use verbose <err> values; report registration)

OK

AT+CPAS (query MT status)

+CPAS: 5 (MT is asleep)

OK

AT+CFUN=1 (set MT to full functionality state)

+CME ERROR: SIM PIN required (SIM requests PIN)

AT+CPIN="1234"

+CME ERROR: incorrect password (user entered wrong PIN)

AT+CPIN="4321"

OK (correct PIN)

AT+COPS=0,0 (ask for automatic operator selection and registration)

OK

+CREG: 1 (registered in the network)

AT+COPS?

+COPS: 0,0,"RADIOLINJA" (get the operator name)

OK

AT+CMEC=1,0,0 (take over the keypad, leave display to MT)

OK

AT+CDIS=?;+CIND=? (query display text and indicator formats)

+CDIS: 10,10,10,6,6

+CIND: ("memory",(0‑2)),("call",(0,1)),("data",(0,1)),("roam",(0,1)),

("alpha",(0,1)),("message",(0,1)),("index1",(0‑11)),("index2",(0‑11)),

("index3",(0‑11)),("signal",(0‑5)),("service",(0,1)),("sel1",(0,1)),

("sel2",(0,1)),("sel3",(0,1)),("battchg",(0‑5))

OK

AT+CSCS="IRA" (set TE character set for display text results)

OK

AT+CMER=1,0,2,2,0 (return display text and indicator result codes when

OK in command state, in data mode discard them)

AT+CDIS?;+CIND? (read current state of display texts and indicators)

+CDIS: "",""," 12345","Menu","Memory" (user had pressed number buttons before

+CIND: 1,0,0,0,0,1,0,0,0,3,1,0,0,0,5 TE took control with +CMEC)

OK

AT+CKPD="C",20 (clear main display text '12345' by holding the

OK 'clear' button down two seconds)

+CDEV: 3,"1234" (first only one character deleted)

+CDEV: 3,"" (while holding continues, whole display is cleared)

+CDEV: 1,"RADIOLINJA" (operator name comes to the display)

The start of the previous example could go as follows when MT has already been powered on but is waiting for the PIN:

AT+CMEE=2;+CREG=1 (use verbose <err> values; report registration)

OK

AT+CPAS (query MT status)

+CPAS: 0 (MT is ready to receive commands)

OK

AT+CPIN? (is MT asking passwords?)

+CPIN: SIM PIN (yes, SIM PIN required)

AT+CPIN="4321"

OK (correct PIN)

One of the most regular operations done through the MT user interface is phonebook control. To lessen the workload of the TE, some direct commands for phonebook reading and writing are practical. Command Select Phonebook Memory Storage +CPBS query version returns supported phonebook memories, read version returns current settings, and set version selects the memory. For GSM, the normal storages are SIM, MT and TA.

Read Phonebook Entries (+CPBR) can be used to read either one or many phonebook locations at the same time. A regular phonebook entry consists of three elements: memory index number, the phone number and its alphanumeric equivalent given by the user. Query version of this returns supported index values of the selected memory, and the maximum lengths of the number and alphanumeric elements. The query version of the Write Phonebook Entry command (+CPBW) is similar, but the action version sets or clears an entry in the phonebook. Find Phonebook Entries (+CPBF) can be used to search alphanumeric entries starting with specific string. An example where the whole phonebook of the MT is read, index number four is cleared, and number three is written:

AT+CPBS=?

+CPBS: ("ME","SM") (MT and SIM have phonebooks)

OK

AT+CPBS="ME" (select MT memory)

OK

AT+CPBR=? (read index range and element lengths)

+CPBR: (1‑99),30,30

OK

AT+CPBR=1,99 (read all entries but only the ones set are returned)

+CPBR: 1,"931123456",129,"Ilkka"

+CPBR: 2,"9501234567",129,""

+CPBR: 4,"901234567",129,"Hesari"

OK

AT+CPBW=4;+CPBW=3,"921123456",,"TS" (clear index 4 and write index 3)

OK

Circuit switched fallback (+CCSFB) can be used to control circuit switched fallback operation. Reporting of CSFB related CS paging requests can be switched on or off by +CCSFB=1 and +CCSFB=0. CSFB related CS paging requests are reported with unsolicited result code +CCSFBU. CSFB calls can be automatically accepted or rejected by +CCSFB=2, +CCSFB=3, +CCSFB=4 and +CCSFB=5. CSFB calls can be manually accepted or rejected by +CCSFB=6 and +CCSFB=7. In the example the ME interrogates the current CSFB settings, enables reporting and accepts a CSFB call:

AT+CCSFB=?

+CCSFB: 0 (reporting and automatic acceptance/rejection disabled)

OK

AT+CCSFB=1 (enable reporting)

OK

+CCSFBU: 2,1,12345678,17 (incoming CSFB paging request with clip supplementary service)

AT+CCSFB=6 (accept CSFB call)

OK

\* \* \* End of Changes \* \* \* \*