Password Reset

For password reset functions, conduct implementation in compliant with the followings. It also shall be possible to reset the password without USIM Card

Password Reset Mode Command List

Downlink（TE-->ME）

	Type	
+CGSN		No continuing data
+CSCC=1,PW REQUEST	Cha	Fixed to 1
+CSCC=2,PW REQUEST ,TOKEN	Cha	1,”A4FCD341” (*4)
+CSCC=3,PW RELEASE	Cha	Fixed to 1
+CPWD=PD,PW DEFAULT(*3)	Cha	“PD”,”M5KPd”(*1)
+CPWAC=CHANGE ACKNOWRIGE (*3)	Cha	Fixed to 1

Uplink（ME-->TE）

		Type	
+CSCC:	CHALLENGE	Cha	“random number” (*4)
+CSCC:2	PW REQUEST ACK.	Cha	Fixed to 1
+CME ERROR:	Error No. (*2)	Cha	Ref:TS27.007,9.2
+CPWCP:	PW CHANGE COMPLETE	Cha	Fixed to 1

*1: FC value: PD (Password Default) will be used.

ME shall reset its internal password to the default when receiving +CPWD=”PD”,”M5KPd.”

When receiving a value other than ”M5KPd,” send the error No.3:”operation not allowed” and end the processing.

*2: Error No.

error code table

No.	Supported by:	Meaning
3	ME	operation not allowed
4	ME	operation not supported (*5)

Codes other than above shall not be sent in this mode.

Incoming such codes shall be ignored.

*5: Send toward non-supported commands (all that can’t be identified)

*3: Send the ” +CPWD” command when resetting a password.

Send back ” +CPWAC” if the operation was successful.

CALC

IMEI: Handset serial number

*4 e.g. :IMEI=33021200123456 (Excluding Check Digit)

:RND=A5 03 BF 66

330212 + 00 + 123456

6digits 2digits 6digits

= 453668 (dec)

= 006EC24 (hex)

= FFF913DB (hex): Reverse the above

+ A503BF66

1 A4FCD341 (hex): Return the low 4 bytes in TOKEN

*Note

Handsets that support +CLAC shall exclude the commands defined in these specifications from the list display by +CLAC

Timer

T01: 1sec

T02: 500msec

T11: 1sec

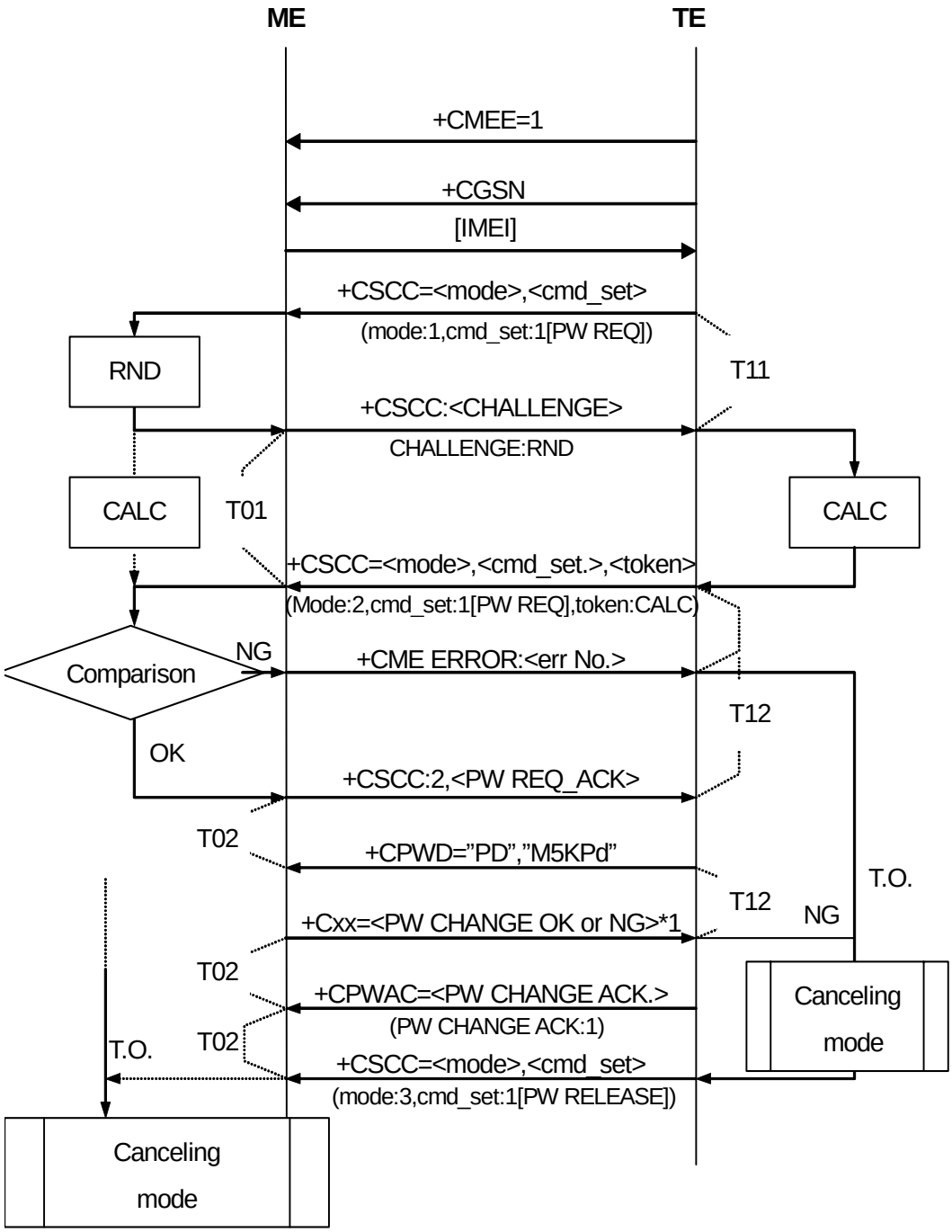
T12: 500msec

Password reset mode in

Password reset mode in shall be established when receiving CSCC=1,1 after IMEI information is sent responding to CGSN.

This shall not apply in the case where USB level release is made after receiving CGSN.

Normal Sequence



*1: Send AT+CPWCP:1 toward +Cxx COMPLETE(OK)

Send AT+CME ERROR:3 toward ERROR(NG)

*Result of OK from ME is omitted on this sequence for a space reason.

* In the normal sequence, ME shall send +CME ERROR error No.3:”operation not allowed,” should it receive +CPWD=<PW DEFAULT> when TE is not notified of IMEI information. ME determines whether or not IMEI information is sent to TE according to whether the handset is turned on or off.
* ME shall cancel the mode autonomously when time is up without a response from TE after identification is finished.
* ME counts the number of wrong +CPWD=<PW DEFAULT> received and record it. After the number reaches five in total, ME shall send the error No.3 even when receiving a proper +CPWD=<PW DEFAULT> from TE.
  Therefore, the maximum value of the counter is five. ME shall send the error No.3 toward the sixth +CPWD=PW request and thereafter regardless of the value.
  The error counter shall be reset when ME is turned off/on.