



Technical Document

SOFTWARE SIMLCK FUNCTIONALITY
MFW/BMI HIGH LEVEL DESIGN

Document Number:	xxxx.xxx.xx
Version:	0.7
Status:	Draft
Approval Authority:	
Creation Date:	2005-Mar-06
Last changed:	2015-Mar-08 by Leelavathi P
File Name:	hld_vle5_smlk_bmi_mfw_ver_0_7.doc

Important Notice

Texas Instruments Incorporated and/or its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products, software and services at any time and to discontinue any product, software or service without notice. Customers should obtain the latest relevant information during product design and before placing orders and should verify that such information is current and complete.

All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment. TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI products, software and/or services. To minimize the risks associated with customer products and applications, customers should provide adequate design, testing and operating safeguards.

Any access to and/or use of TI software described in this document is subject to Customers entering into formal license agreements and payment of associated license fees. TI software may solely be used and/or copied subject to and strictly in accordance with all the terms of such license agreements.

Customer acknowledges and agrees that TI products and/or software may be based on or implement industry recognized standards and that certain third parties may claim intellectual property rights therein. The supply of products and/or the licensing of software does not convey a license from TI to any third party intellectual property rights and TI expressly disclaims liability for infringement of third party intellectual property rights.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products, software or services are used.

Information published by TI regarding third-party products, software or services does not constitute a license from TI to use such products, software or services or a warranty, endorsement thereof or statement regarding their availability. Use of such information, products, software or services may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI. No part of this document may be reproduced or transmitted in any form or by any means, electronically or mechanically, including photocopying and recording, for any purpose without the express written permission of TI.

Change History

Date	Changed by	Approved by	Version	Status	Notes
2005-Mar-06	Leelavathi P		0.1	Initial Draft	1
2005-Mar-14	Leelavathi P		0.2	Initial Draft	2
2005-Apr-01	Leelavathi P		0.3	Initial Draft	3
2005-04-11	Samir Amberkar		0.4	Draft	4
2005-04-11	Samir Amberkar		0.5	Draft	4
2005-04-15	Leelavathi P		0.6	Draft	6
2005-04-18	Leelavathi P		0.7	Draft	7

Notes:

1. Initial Draft
2. Added features UI for ME unblocking, UI for Failure Counter Reset and UI for getting maximum and current Failure counter values
3. Incorporated the review comments from Oleksiy and TA
4. Incorporating review comments by T&A and TI
5. Incorporating review comments by T&A and TI
6. Incorporating review comments by T&A and TI
7. Incorporating review comments by T&A and TI

Table of Contents

1	Introduction	6
2	Scope	7
3	Structure of MMI/ACI/SIMLCK.....	8
4	Design.....	9
4.1	UI for ME locking to NW, NS, SP, CP, SIM	9
a)	With correct password:.....	9
b)	With wrong password:	10
4.2	UI for ME unlocking NW, NS, SP, CP, SIM	11
a)	With correct password:.....	11
b)	With wrong password:	12
c)	With all attempts failed:	13
4.3	UI for password changing of NW, NS, SP, CP, SIM	14
a)	With correct old password:.....	15
b)	With wrong old password:.....	16
4.4	UI for status check of NW, NS, SP, CP, SIM	17
4.5	Personalization check (during Boot-up).....	18
a)	With correct password:	18
b)	With wrong password:	20
c)	With all attempts failed:	21
4.6	UI for getting Failure Counter	23
4.7	UI for resetting Failure Counter	25
5	Annexure A “Example for Customer-MMI development”	27
5.1	Timer Management	27
5.2	Reset FC Management	27
6	Annexure B “Terms and Definitions”	28

List of References

Sr. No	Document/File name	Version
1.	3GPP TS 22.022 Personalization of ME	V3.2.1 (2002-06)
2.	3GPP TS 27.007 AT Command set for User Equipment	V 3.13.0 (2003-03)
3.	3GPP TS 11.11 Mobile Equipment (SIM-ME) Interface	V 8.9.1 (2003-06)
4.	ME Personalization Requirements - SIM-ME-LOCK VLE SIM-ME-LOCK on VLE5 Handsets	0.2
5.	ME Personalization Requirements - SIM-ME-LOCK SIM-ME-LOCK on Alcatel Handsets	0.1
6.	TA_SIM_Lock_TR_Frozen.xls	
7.	ACI-ME Personalization – Interface Description	Draft

1 Introduction

ME Personalization module implement the ME Personalization functionality as defined by the standard 22022-321. In the TI context, this functionality is implemented at the ACI layer. Also there will be implementation in the MMI layer for user interface changes mainly to check the ACI functionality.

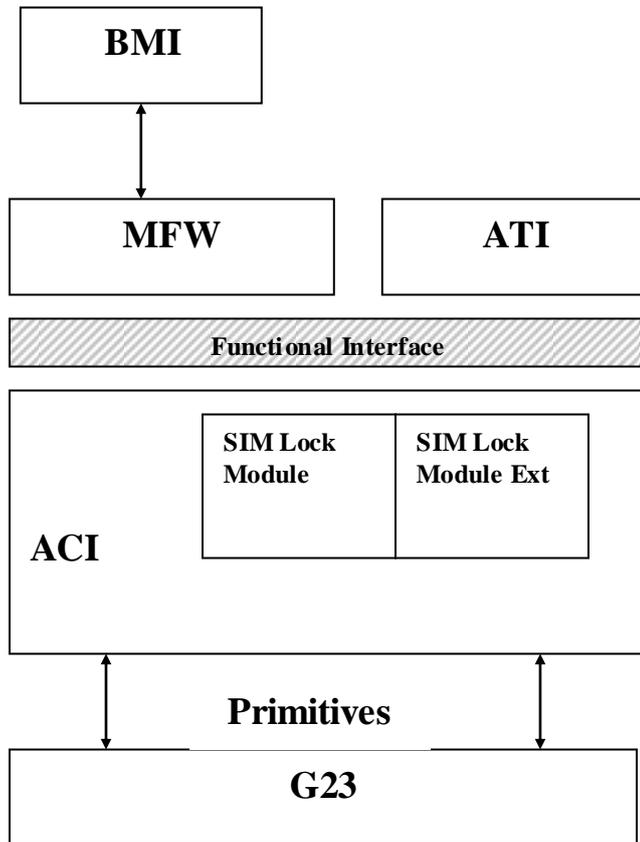
2 Scope

This document presents the MFW and BMI part of High level design for ME Personalization (SIM Lock) functionality.

It covers customization for the following features:

1. UI for Category locking to NW, NS, SP, CP, SIM
2. UI for Category unlocking NW, NS, SP, CP, SIM
3. UI for password changing of NW, NS, SP, CP, SIM locks
4. UI for status check of NW, NS, SP, CP, SIM locks
5. Personalization check -> during Boot-up
6. UI for getting Failure Counter
7. UI for resetting Failure Counter

3 Structure of MMI/ACI/SIMLCK



4 Design

The various scenarios related to ME Personalization (SIM Lock) are described below in the form of Message Sequence Charts between BMI, MFW and ACI layers.

4.1 UI for ME locking to NW, NS, SP, CP, SIM

- MFW will provide an interface for the user to select a category to be locked.
- If the selected category is not locked then the user will be prompted to enter the password (control key) for locking the category.

a) With correct password:

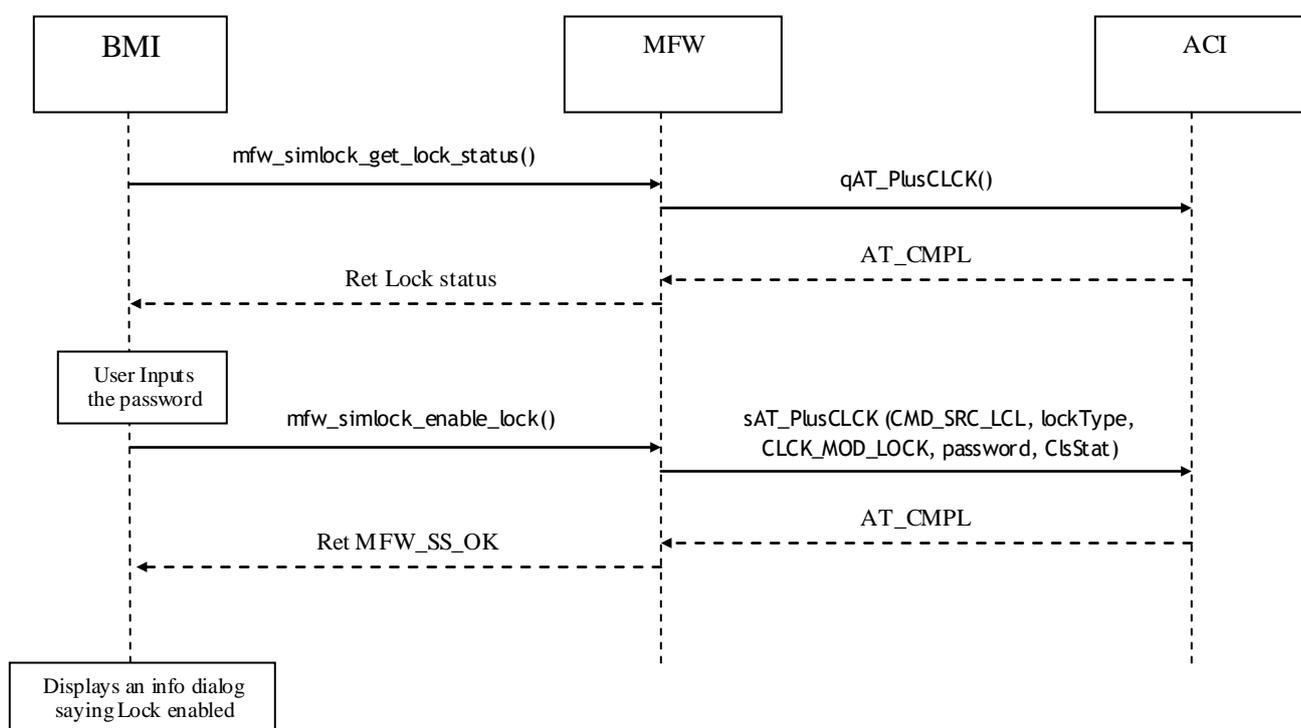


Fig 1

1. BMI queries current status of the selected lock.

2. MFW replies with status for the queried lock (whether Locked or Unlocked).
3. If ME is not blocked and the status is locked, an information dialog saying, “Category already locked” is displayed to the user.
4. If ME is not blocked and the status is not locked, the user is prompted to enter the password
5. The user will enable the lock by entering the correct password for the selected lock.
6. The mfw_simlock_enable_lock() is called by BMI and in turn sAT_PlusCLCK () is called by MFW with the mode set to CLCK_MOD_LOCK.
7. The result of enabling lock is returned by ACI, AT_CMPL indicates the successful enabling of the lock.

b) With wrong password:

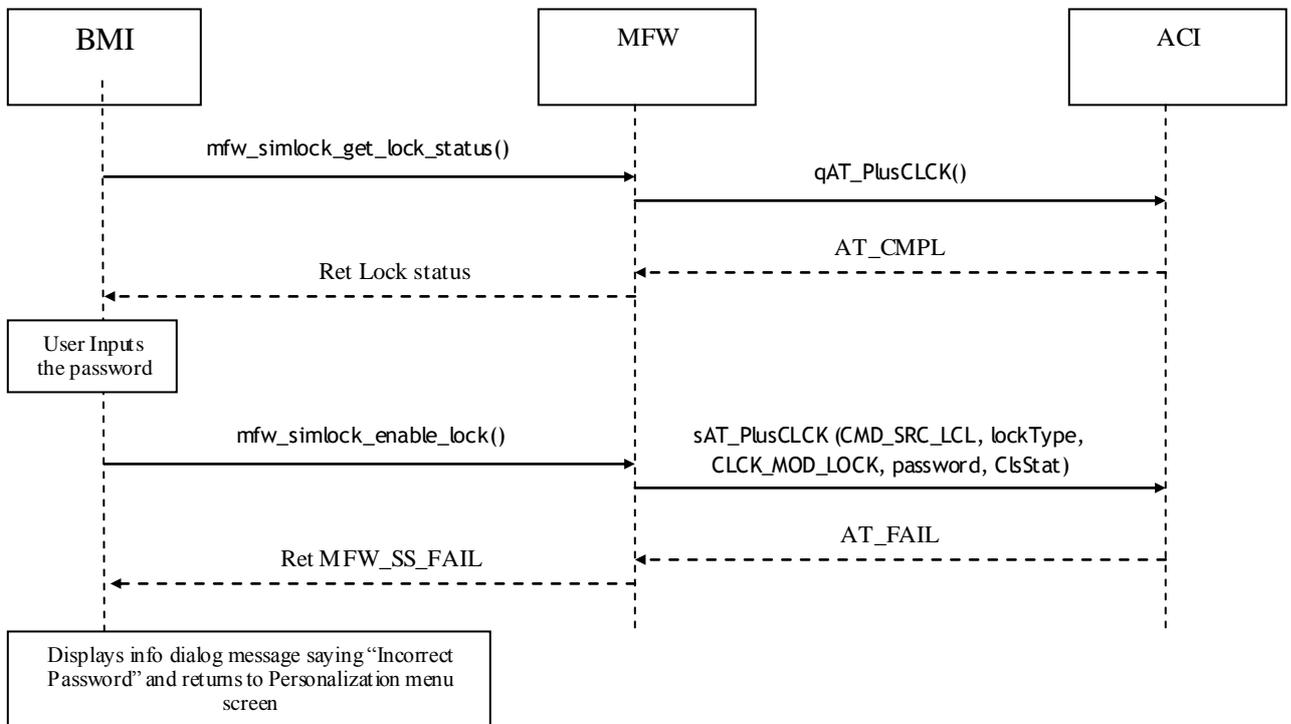


Fig 2

1. BMI queries current status of the selected lock.
2. MFW replies with status for the queried lock (whether Locked or Unlocked).
3. If ME is not blocked and the status is locked, an information dialog saying, “Category already locked” is displayed to the user.
4. If ME is not blocked and the status is not locked, the user is prompted to enter the password
5. If the user enters the wrong password the ACI returns the AT_FAIL.
6. An information screen is displayed informing incorrect password and taken back to the Personalization menu screen.

4.2 UI for ME unlocking NW, NS, SP, CP, SIM

- MFW will provide an interface for the user to select a category to be unlocked.
- If the selected category is locked then the user will be prompted to enter the password (control key) for unlocking the category.

a) With correct password:

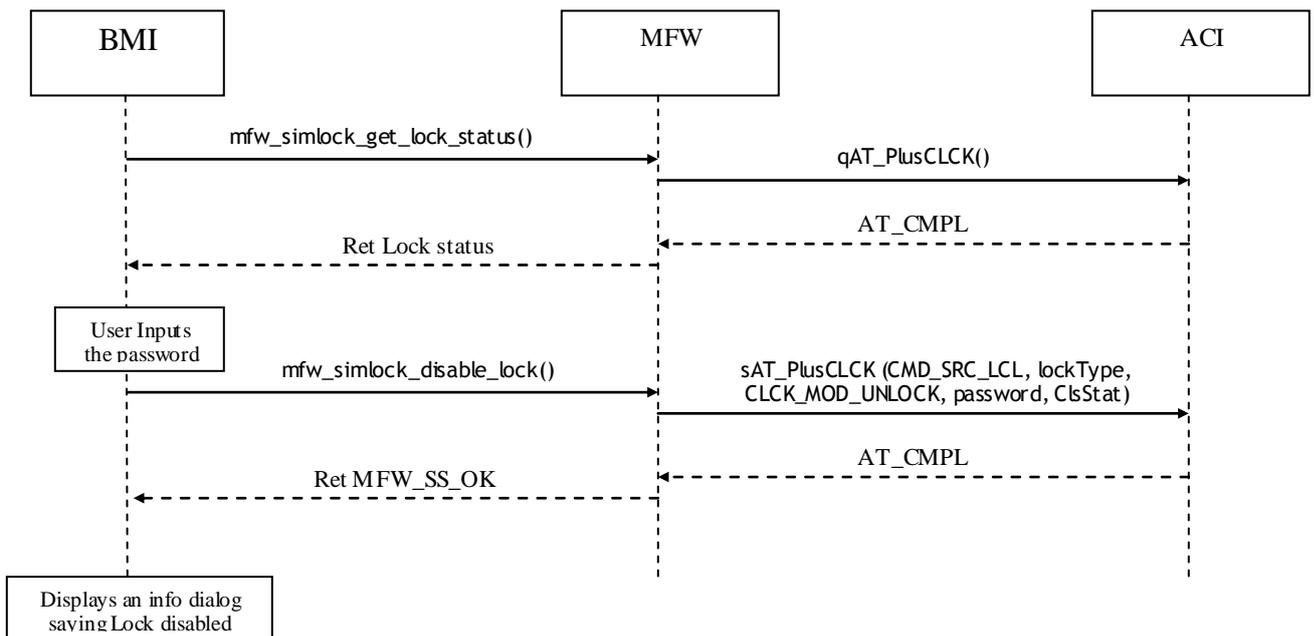


Fig 3

1. BMI queries current status of the selected lock.
2. MFW replies with status for the queried lock (whether Locked or Unlocked).
3. If ME is not blocked and the status is not locked, an information dialog saying, “Category already unlocked” is displayed to the user.
4. If ME is not blocked and the status is locked, the user is prompted to enter the password
5. The user will disable the lock by entering the correct password for the selected category. The `mfw_simlock_enable_lock()` is called by BMI and in turn `sAT_PlusCLCK ()` is called by MFW with the mode set to `CLCK_MOD_UNLOCK`.
6. The result of disabling lock is returned by ACI, `AT_CMPL` indicates the successful disabling of the lock.

b) With wrong password:

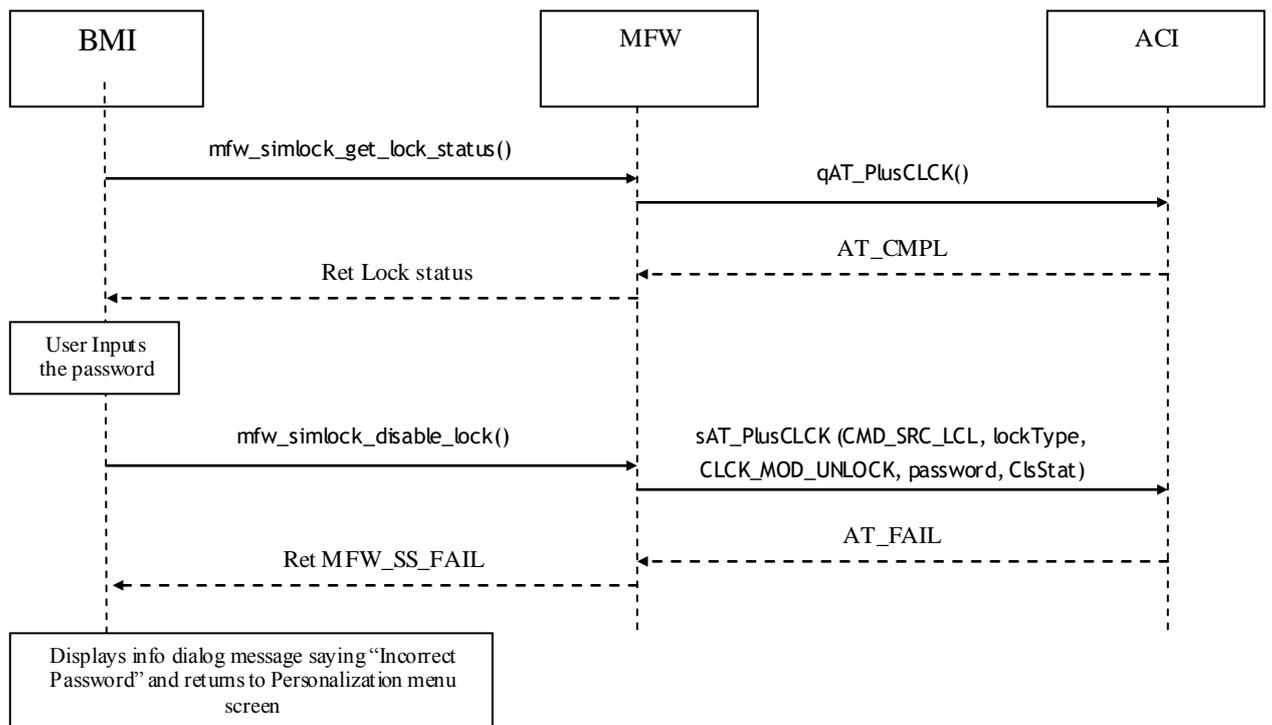


Fig 4

1. BMI queries current status of the selected lock.
2. MFW replies with status for the queried lock (whether Locked or Unlocked).
3. If ME is not blocked and the status is locked, the user is prompted to enter the password
4. If the user enters the wrong password the ACI returns the AT_FAIL.
5. An information screen is displayed informing incorrect password and taken back to the Personalization menu screen. (BMI can as well request FC and FCmax value from ACI using qAT_percentMEPD and display it to user as “n tries left” before moving on to personalization menu screen)

c) With all attempts failed:

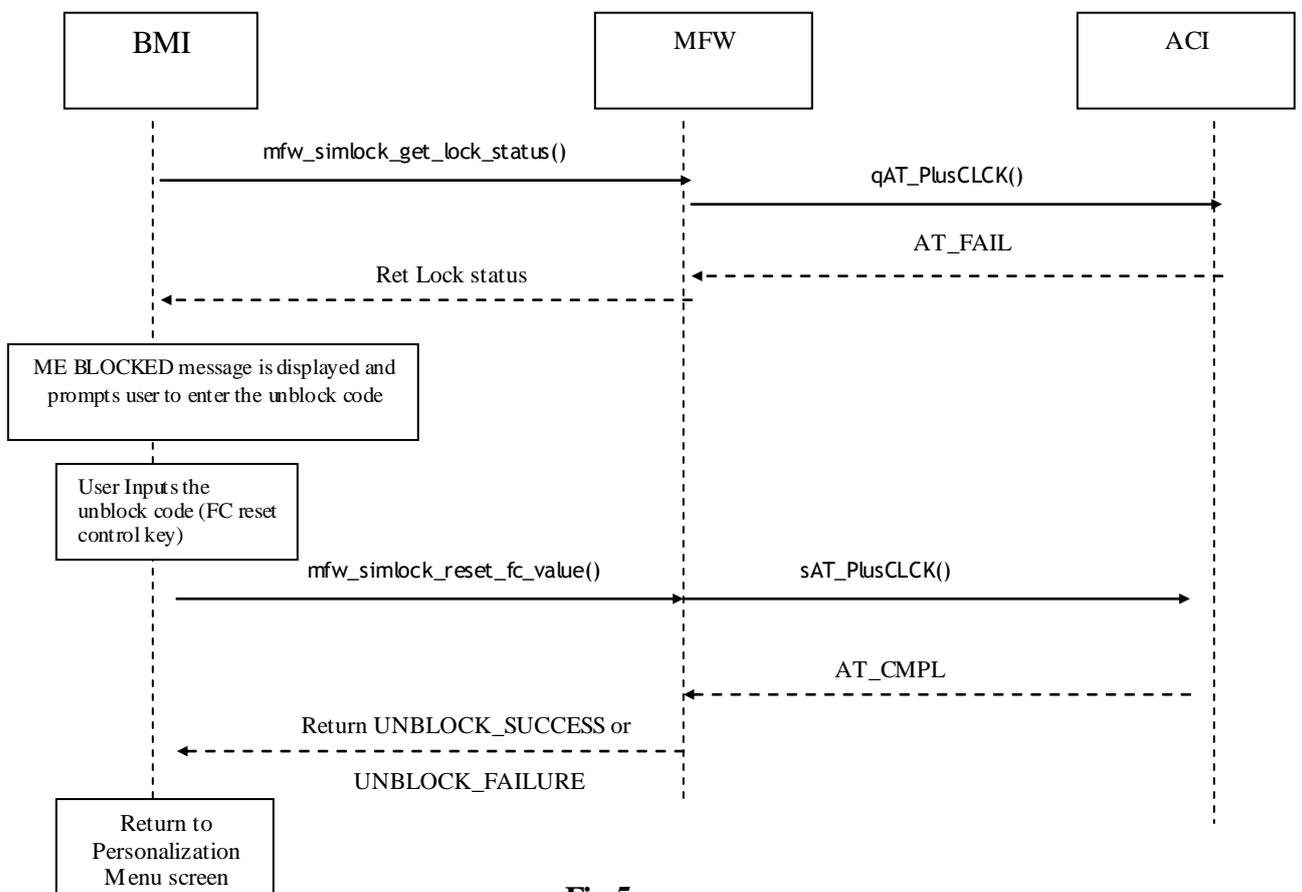


Fig 5

1. If the number of attempts to deactivate the lock exceeds the total number of allowed attempts, a blocked message will be displayed and prompt for unblock code entry is displayed every time the user attempts to do any operations on ME.
2. If the valid unblock code is entered, the ME will be unblocked else the control returns to Unblock code entry screen
3. ME will allow only emergency calls to be made in the blocked state.

4.3 UI for password changing of NW, NS, SP, CP, SIM

- MFW will provide an interface for the user to select a category whose password needs to be changed.
 - The user will be prompted to enter the old password and new password (twice).
1. BMI queries current status of the selected lock.
 2. MFW replies with status for the queried lock (whether Locked or Unlocked).
 3. If ME is locked and not blocked, the user will not be allowed to change the password. An information dialog saying “Lock Enabled” will be displayed.
 4. If ME is not locked or not blocked, the user is prompted to enter the old password and the new password (twice)
 5. The old password will be changed to the new password by calling the API sAT_PlusCPWD ().
 - on successful completion, sAT_PlusCPWD return AT_CMPL; user will be informed of the successful completion (refer fig 6)
 - if failure scenario, sAT_PlusCPWD return AT_FAIL; user will be informed of the failure (refer fig 7).

a) With correct old password:

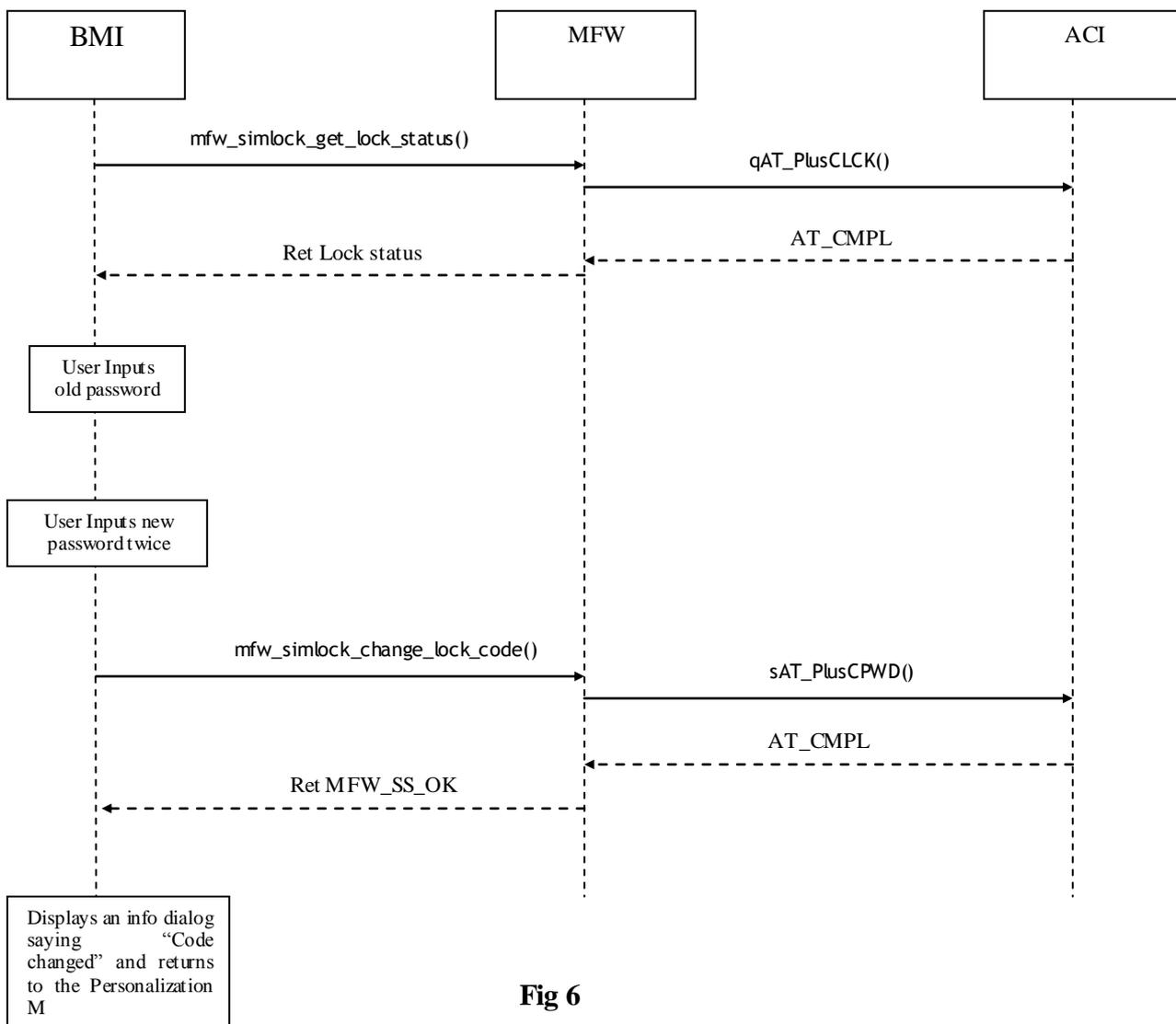


Fig 6

b) With wrong old password:

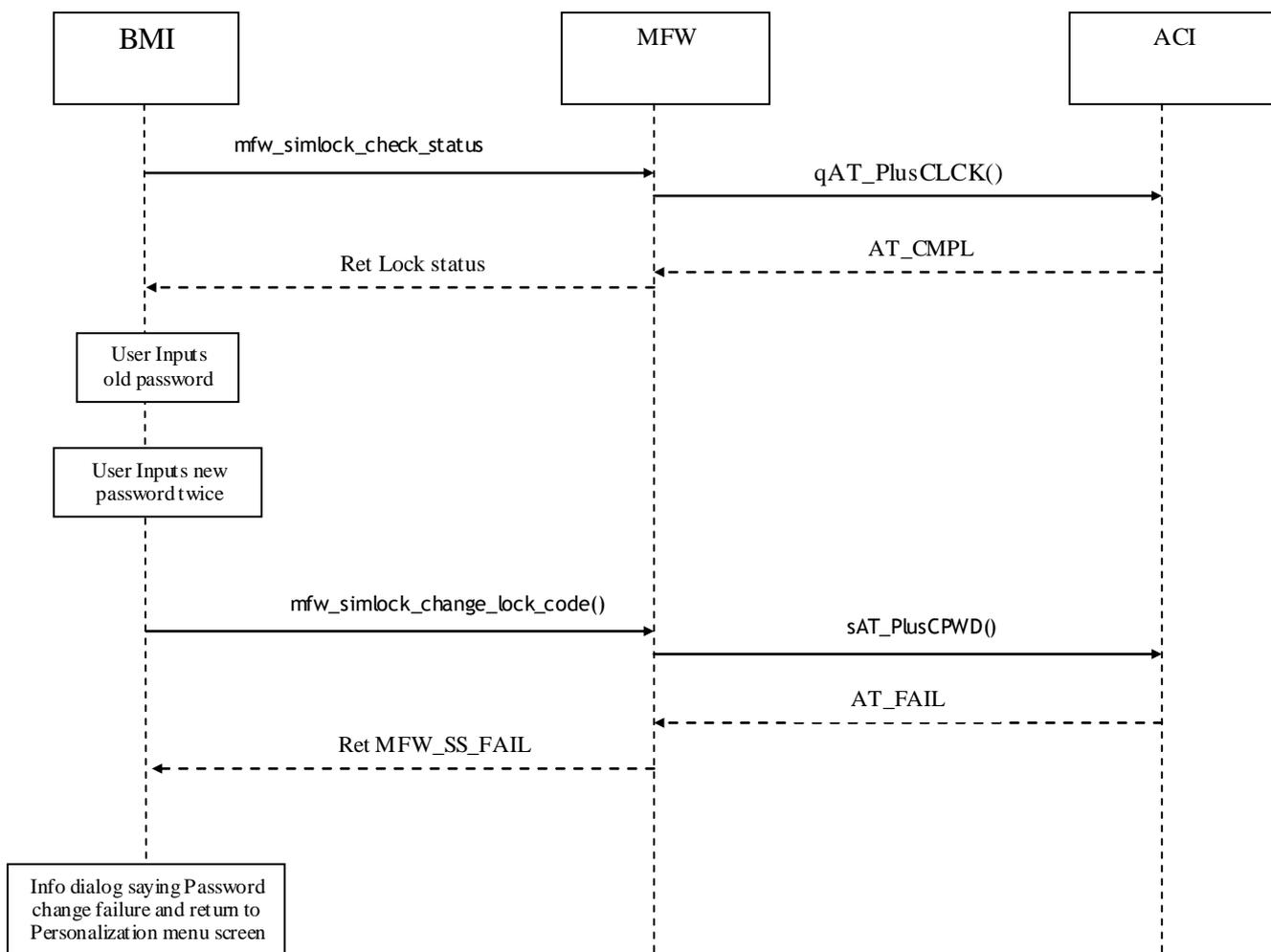


Fig 7

4.4 UI for status check of NW, NS, SP, CP, SIM

- MFW will provide an interface for the user to select a category whose status has to be checked.

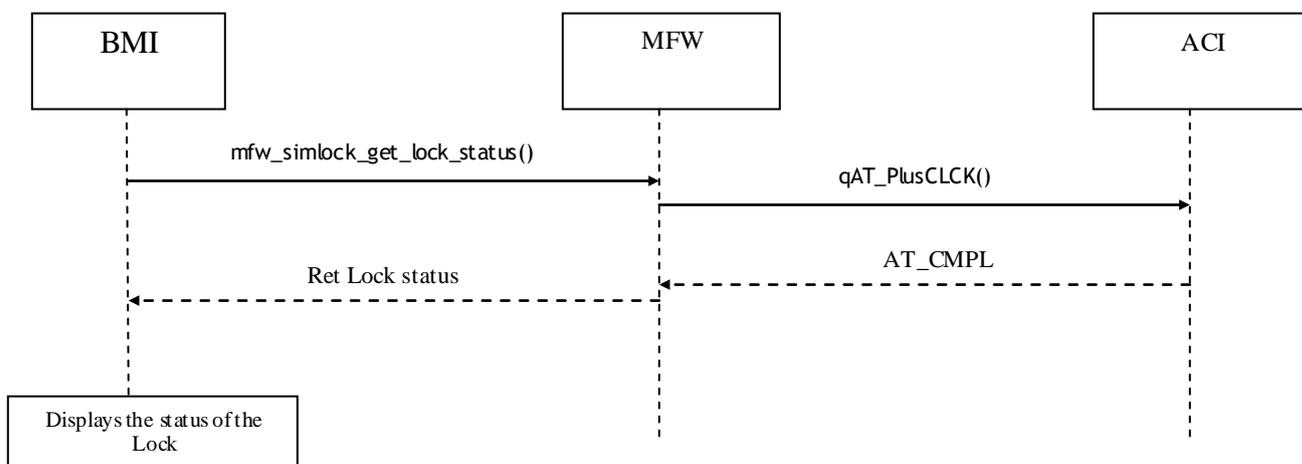


Fig 8

1. BMI queries current status of the lock.
2. MFW replies with status for the queried lock (whether Locked or Unlocked).
3. An information screen is displayed informing the status of the lock of the category selected.

4.5 Personalization check (during Boot-up)

a) With correct password:

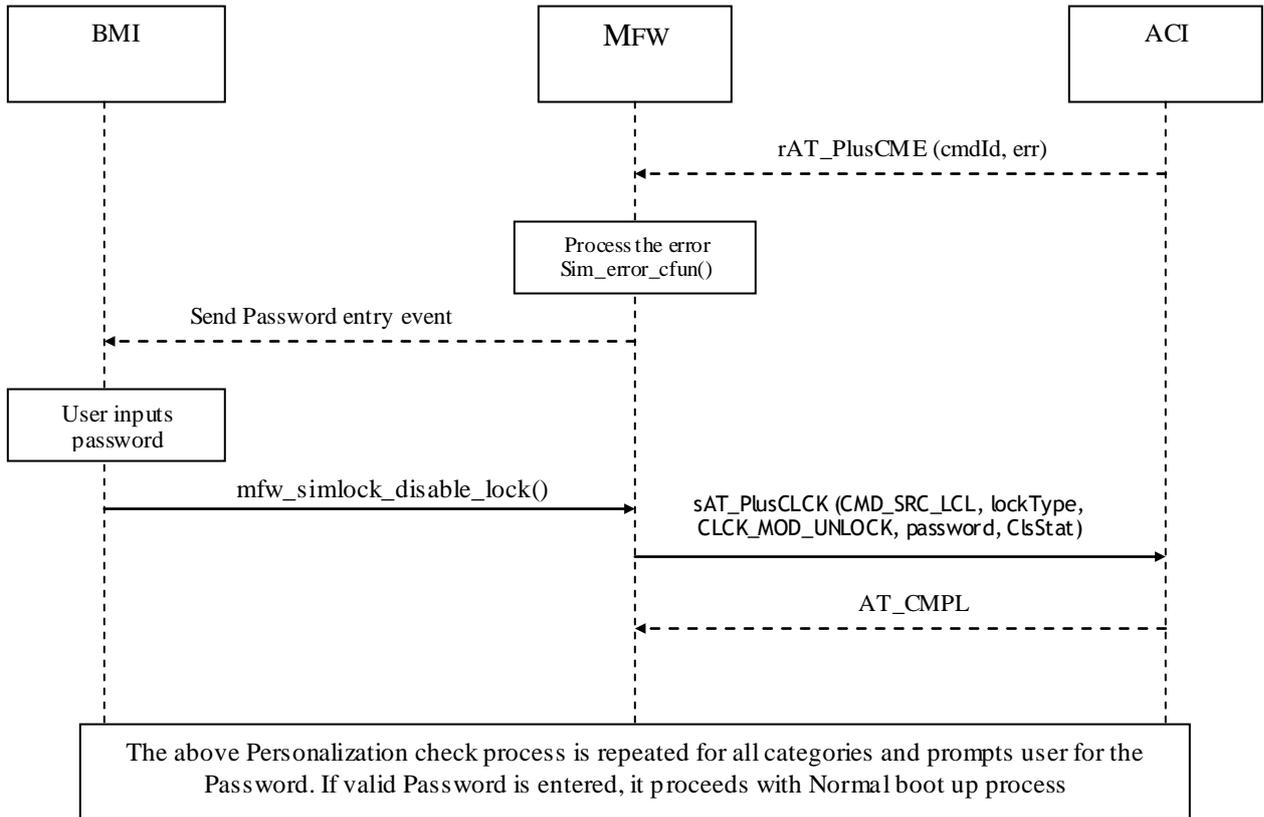


Fig 9

1. When ACI comes across with the SIM_Lock enabled for any one of the locks, it will send an indication to the BMI by placing a call to the rAT_PlusCME () with one of the error number, which corresponds to the lock enabled
 - CME_ERR_NetworkPersPinReq,
 - CME_ERR_NetworkSubsetPersPinReq,

- CME_ERR_ProviderPersPinReq,
 - CME_ERR_CorporatePersPinReq
 - CME_ERR_PhSimPinReq.
2. The function `sim_error_cfun ()` is called with the error number, which indicates the lock is been enabled and password is required for the same.
 3. The MFW sends an event to BMI for Password entry.
 4. The BMI then calls the MFW interface `mfw_simlock_disable_lock ()` to unlock the locked category.

Note: "If it is desired not to unlock the category but to verify the control key during boot up check, the customer MMI shall use AT+CPIN (mfw_simlock_verify_pin)"

5. On entry of valid password, the personalization check process continues for all types of categories. If any of the category types are enabled, then the user is prompted to enter the password for that category.
6. When all valid passwords are entered for the locked categories, BMI proceeds with the normal boot up of the phone.
7. When phone is rebooted (with same or different SIM inserted), steps 1 through 6 will be followed

b) With wrong password:

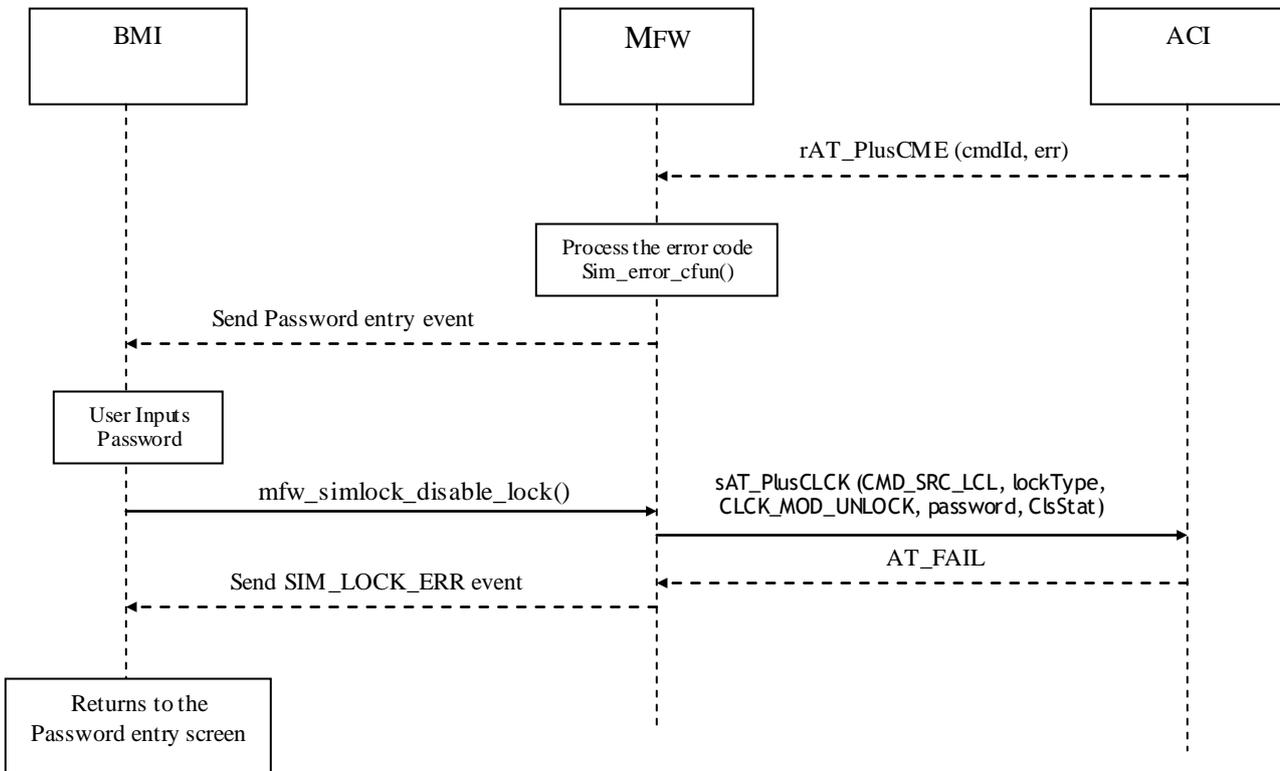


Fig 10

1. The function `sim_error_cfun ()` is called with the error number, which indicates the lock is been enabled and password is required for the same.
2. The MFW sends an event to BMI for Password entry.
3. The BMI then calls the MFW interface `mfw_simlock_disable_lock ()` to unlock the locked category.

Note: "If it is desired not to unlock the category but to verify the control key during boot up check, the customer MMI shall use AT+CPIN (mfw_simlock_verify_pin)"

4. On entry of wrong password, ACI returns `AT_FAIL` and MFW will send an event to BMI to enter the password again.

c) With all attempts failed:

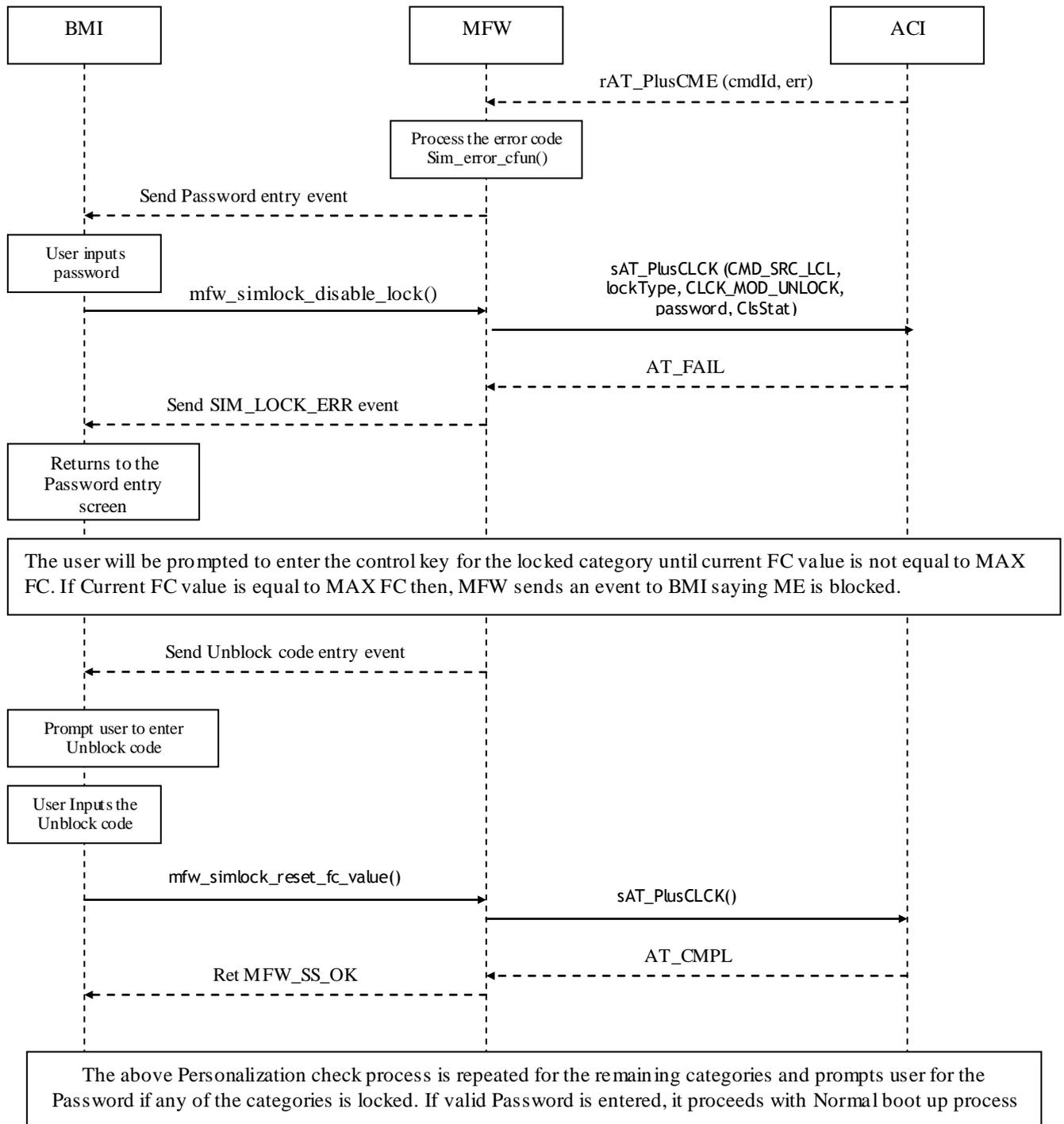


Fig 11

1. The function `sim_error_cfun ()` is called with the error number, which indicates the lock is been enabled and password is required for the same.
2. The MFW sends an event to BMI for Password entry.
3. The BMI then calls the MFW interface `mfw_simlock_disable_lock ()` to unlock the locked category.

Note: "If it is desired not to unlock the category but to verify the control key during boot up check, the customer MMI shall use AT+CPIN (mfw_simlock_verify_pin)"

4. On entry of wrong password, ACI returns `AT_FAIL` and MFW will send an event to BMI to enter the password again.
5. The user will be prompted to enter the control key for the locked category until current FC value is not equal to `MAX FC`.
6. If Current FC value is equal to `MAX FC` then, MFW sends an event to BMI saying ME is blocked.
7. The user is prompted to enter the unblocking code
8. If the user enters incorrect password, the user will be prompted to enter the unblocking code
9. Else if the user enters correct unblocking code, the personalization check process continues for the remaining types of categories. If any of the category types are enabled, then the user is prompted to enter the password for that category.
10. When all valid passwords are entered for the locked categories, BMI proceeds with the normal boot up of the phone else steps 2 through 9 will be followed

4.6 UI for getting Failure Counter

BMI will provide an interface for the user to:

- Get Maximum Failure Counter
- Get the current Failure Counter Value

a) Get Failure Counter value

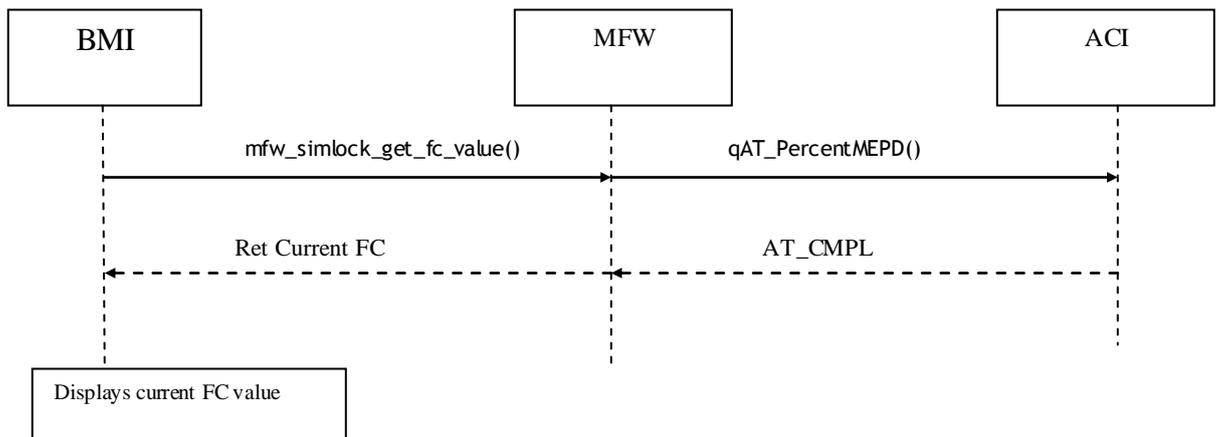


Fig 12

1. MFW queries ACI for the current value of FC.
2. If the request is successful then, ACI returns `AT_CMPL` with the current value of FC.
3. BMI displays an information screen showing the current FC value

b) **Get Maximum Failure Counter value**

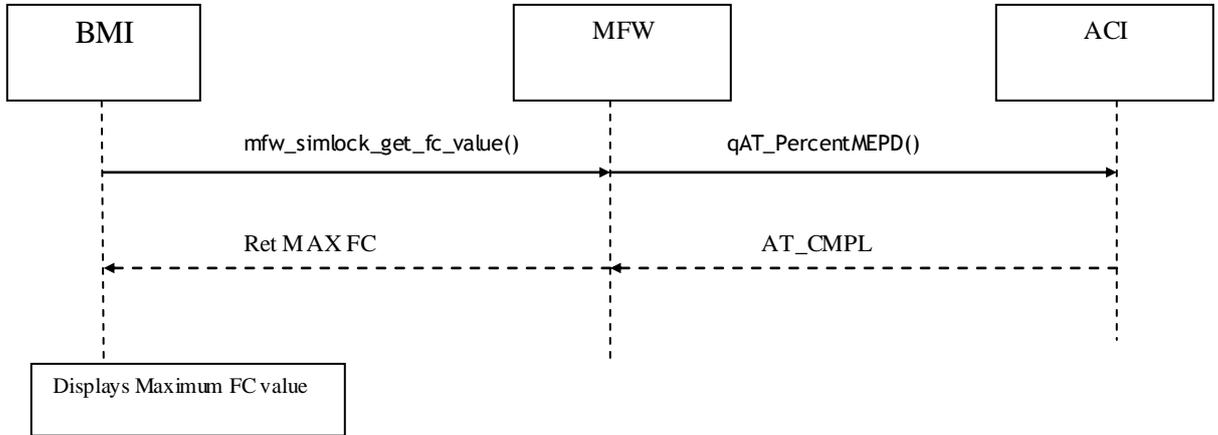


Fig 13

1. MFW queries ACI for the Maximum value of FC.
2. If the request is successful then, ACI returns AT_CMPL with the maximum value of FC.
3. BMI displays an information screen showing the Maximum FC value

4.7 UI for resetting Failure Counter

MFW will provide an interface for the user to reset the Failure Counter

a) Reset Failure Counter- Success

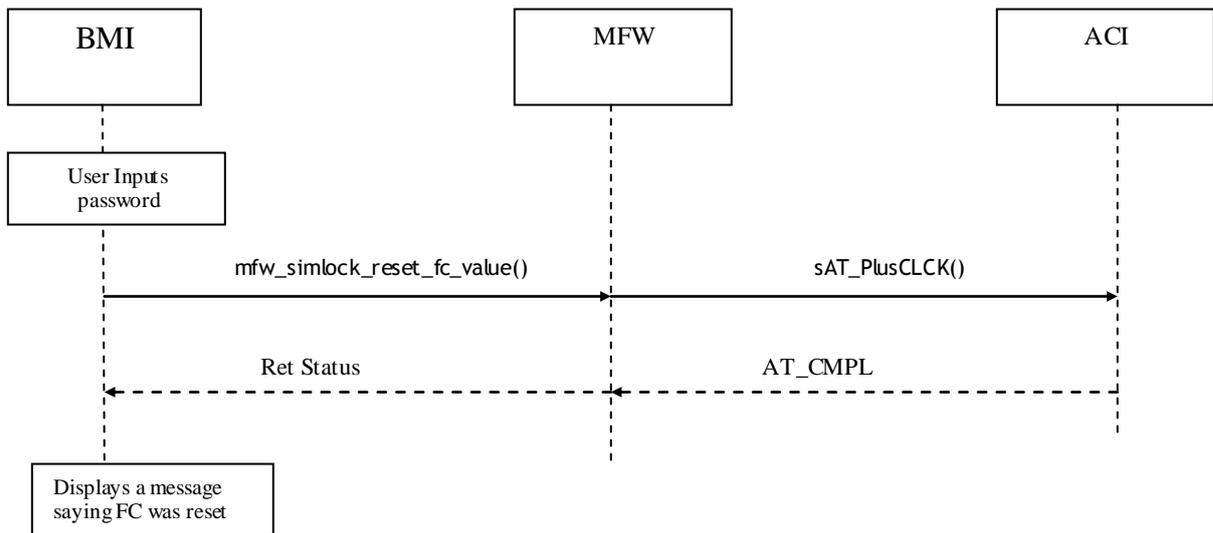


Fig 14

1. BMI prompts the user to enter the password before resetting the FC value.
2. If the password is correct then a request is sent to ACI to reset FC value.
3. If password is correct, ACI returns AT_CMPL
4. BMI displays an information screen saying FC has been reset

b) Reset Failure Counter – Failure

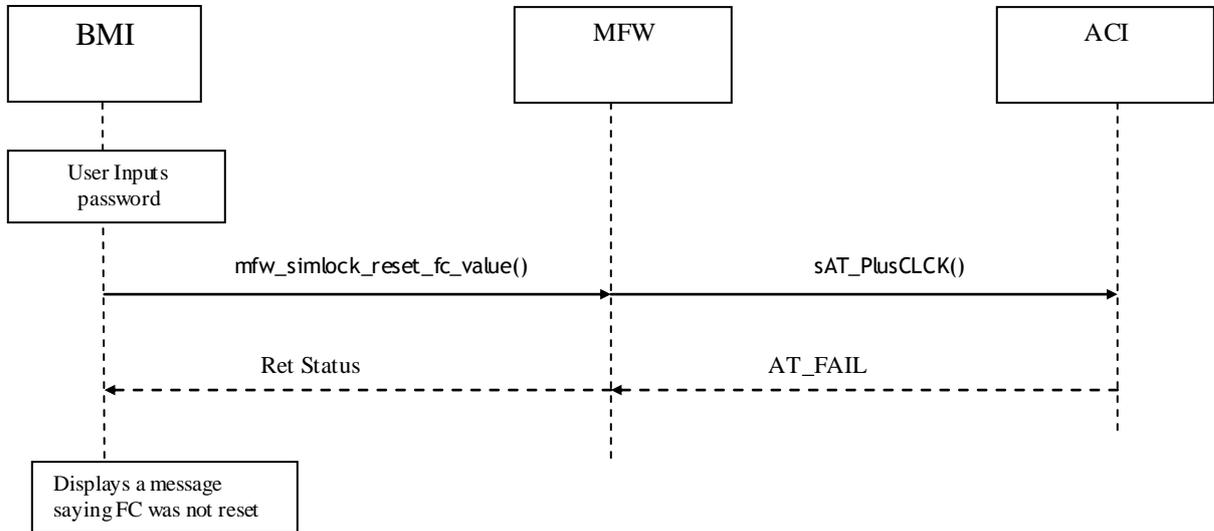


Fig 15

1. BMI prompts the user to enter the password before resetting the FC value.
2. If password is incorrect, ACI returns AT_FAIL
3. BMI displays an information screen saying incorrect password will be displayed and return to Personalization Menu screen.

5 Annexure A “Example for Customer-MMI development”

5.1 Timer Management

- Initialize timer_value to 30 seconds. Set a timeout_flag to TRUE
- While unlocking a category, if the user enters wrong password, then start the timer and set the timeout_flag to FALSE.
- On time out, stop the timer, set the timeout_flag to TRUE and increment the current timer_value by 30 seconds.
- The maximum value of timer_value will be 1800 seconds.
- If the user enters the correct password, then set the timer_value to 30 seconds and timeout_flag to TRUE.
- On the basis of the timer_flag (set to TRUE), the user will be allowed to enter the unlocking password

5.2 Reset FC Management

- Assuming that Secure Driver is maintaining a counter for the attempts made for Reset FC, MFW shall query ACI to get the current value of counter for Reset FC.
- When phone is in blocked state or if the user selects the “Reset FC” option from the menu, password entry screen is displayed. Note that "failed reset counter" can be reset even if it has not reached its maximum value.
- If the user enters correct password, then the current value of counter for Reset FC will be set to zero.
- If the user enters wrong password, then display “<n> tries left” for the user by querying ACI to get the current value of counter for Reset FC. <n> denotes the current value of counter for Reset FC
- When the number of tries left is equal to zero, BMI will display an information dialog saying, “Number of tries left is zero, phone blocked permanently, contact your dealer”.
- ME will allow only emergency calls in this blocked state.

6 Annexure B “Terms and Definitions”

Terms:

ACI Application Control Interface

NW Network

NS Network Subset

SP Service Provider

CP Corporate (Category)

SIM Subscriber Identity Module

MMI Man Machine Interface

BMI Basic MMI

MFW MMI Framework

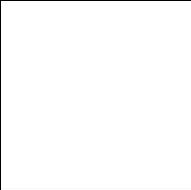
SIMLCK SIM Lock

UI User Interface

ME Mobile Equipment

FC Failure Counter

ATI AT Command Interpreter



Definitions:

Category Lock: Is the process of storing information in the ME and activating the procedures which verify this information against the corresponding information stored in the SIM/USIM whenever the ME is powered up or a SIM/USIM is inserted, in order to limit the SIM/USIMs with which the ME will operate.

Category Unlock: Is the process of deactivating the personalisation so that the ME ceases to carry out the verification checks.

ME Blocked: To limit the number of failed attempts during unlocking the category, a failure counter can be managed by the handset. Once the maximum limit has been reached, the handset is temporarily blocked and only emergency calls are allowed.

To unblock the temporarily blocked handset, entering a special “reset counter” key shall reset the failure counter. Once the numbers of tries to reset the failure counter (for wrong control key entry) has reached the maximum limit, the handset is definitely blocked and must be returned to factory for unblocking