Technical Documentation

SixTIes Security Code Low Level Design specification ACI

Department:	WTBU - Cellular Systems		
Creation Date:	2004-08-19		
Last Modified:	2004-09-21 by Saeed Yakehpar		
ID:	8462.738.04.002	Version:	002
Status:	Submitted	ECCN:	Not Applicable

0 Document Control

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 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 do 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, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of TI.

0.1 Export Control Statement

Recipient agrees that it will not knowingly export or re-export, directly or indirectly, any product or technical data (as defined by the U.S, EU and other Export Administration Regulations) including software, or any controlled product restricted by other applicable national regulations, received from Disclosing party under this Agreement, or any direct product of such technology, to any destination to which such export or re-export is restricted or prohibited by U.S or other applicable laws, without obtaining prior authorisation from U.S. Department of Commerce and other competent Government authorities to the extent required by those laws. This provision shall survive termination or expiration of this Agreement.

According to our best knowledge of the state and end-use of this product or technology, and in compliance with the export control regulations of dual-use goods in force in the origin and exporting countries, this

technology is classified as given on the front page.

This product or technology may require export or re-export license for shipping it in compliance with certain countries regulations.

0.2 Document History

Date	Version	Status	Author
2004-08-19	001	Draft	Saeed Yakehpar
2004-09-21 Initial version. 001	002	Updates for Release 2004-09-10	Saeed Yakehpar

0.3 References, Abbreviations, Terms

Table of Contents

1 Introduction

From Customer:

We must be able to set/verify the security code and to know if it is required at start-up or not.

Access to the security code by SixTIes components is managed by the TSY plugin and provides the following services:

Change security code

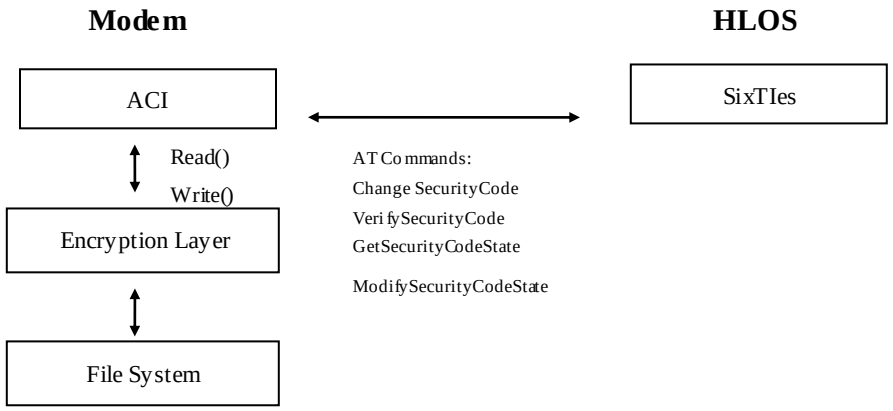
Verify security code

Get security code state (active or not)

Modify security code state (active or not)

One requirement is that the security code can be returned to its default value. If the security code is stored in the GSM FFS then restoring the original GSM FFS will achieve this.

The understanding of this requirement is as follows:



For this functionality we need two new AT commands

%SECP to Change / Verify the password, <security code>

%SECS to Modify / Query the security code state, <state>

The <state>, <security code>, Password length along with the original <security code> i.e.12345 will need to be retained by the ACI in the GSM FFS. (Ref Sec 3.2.3)

2 Interface changes

2.1 %SECP parameter command syntax

Command	Possible response(s)
%SECP= [<security code>[,<new security code>]]	+CME ERROR
%SECP=?	

2.2 %SECS parameter command syntax

Command	Possible response(s)
%SECS= <state>,<security code>	+CME ERROR
%SECS?	%SECS: <state>
%SECS=?	%SECS: (list of supported <state>s)

Defined values

<state>:

0 The security code is not required

1 The security code is required

<security code>:

<security code> ,<new security code> string type: <security code> shall be the same as password specified for the facility using the command %SECP for change of password and <new security code> is the new password; passwords will have length = 5 as default but the length is programmable via the FFS data (Ref Sec 3.2.3)

3 Proposed Low Level Design.

3.1 Interface Changes

The new command %SECP and %SECS will be defined as described above.

3.2 ATI Modifications.

3.2.1 New Functions:

-setatPercentSECP(). It will handle the %SECP command.

-setatPercentSECS (). It will handle the %SECS command.

3.2.2 Affected Global variables:

The ATI array "cmds", in the file ati_cmd.c, will be updated with the new functions as follow:

SetatPercentSECP ()

SetatPercentSECS ()

quetatPercentSECS ()

aci_cmh.h:

Addition of Ids AT_CMD_P_SECP and AT_CMD_P_SECS will be necessary to type T_ACI_AT_CMD for call to the functions above.

Typedef T_ACI_SECS_STA will be defined to represent the security states possible.

3.2.3 New Global variables in FFS:

The current <security code>, the original <security code> i.e.12345, <state> and length of the security code will be retained by the ACI in the GSM FFS.

Using FFS Dir: "/gsm/MELOCK"

And FFS File: "SecCode"

FFS Variables: State, PWDLength, Cur_code, Org_code using type T_ACI_PERS_MMI_DATAS

The data in SecCode is a follows:

```
T_ACI_PERS_MMI_DATAS MMI_personalisation_status =
{
  0x01,        // State Enabled, MMI access requires Password input
  0x00,        // Count
  0x03,        // Max Count
```

```
  0x05,          // Pwd length
  0x21,0x43,0xF5,    // Original code BCD
  0x21,0x43,0xF5    // Current code BCD
};
```

3.2.3.1 FFS Initialisation

If on power up no FFS directory exists, then the default password ('12345') is utilised as hard coded in the customisation data (Ref Sec 3.2.3).

Upon a password verification action the FFS directory "/gsm/MELOCK/SecCode" will be created by the ACI thus enabling change of password and other MMI blocking procedures.

Copy of the FFS file is included in the following directory:

\\dbgs2\deveng\cc\aci_mmi_intern\programs\TCS_3.x\SixTIes\Technical Docs\GAP 005 Sec

3.2.4 Description of the changes:

Set, Test and Query …atPercentXXX() functions will parse the command line parameters to call cmh layer functionality as below.

setatPercentSECP() will call sAT_PercentSECP().

setatPercentSECS () will call sAT_PercentSECS ().

quetatPercentSECS () will call qAT_PercentSECS()

3.3 CMH Modications

3.3.1 New Functions

These functions carry out the functional counterpart to the AT command.

sAT_PercentSECP()

sAT_PercentSECS()

qAT_PercentSECS()

3.3.2 Encryption

All FFS file system communication will be handled via filename \g23m-aci\aci_ext\aci_ext.c where the customer can add personalised encryption under the ACI_PERSONALISTION_USE_FFS compile switch.

3.4 ACI EXT Modifications

The following ID and functions are added to save and retrieve data from FFS.

typedef T_MMILOCK_STATUS represents the MMILock states.

T_MMILOCK_STATUS aci_ext_personalisation_MMI_verify_password(char *passwd);

T_MMILOCK_STATUS aci_ext_personalisation_MMI_change_password(char *passwd, char *new_passwd);

T_MMILOCK_STATUS aci_ext_personalisation_MMI_get_status();

T_MMILOCK_STATUS aci_ext_personalisation_MMI_set_status(T_MMILOCK_STATUS status);

3.5 Additional Notes

At the moment any number of password retries are allowed.
However in future software releases three attempts for the pin code will be allowed after which the MMI will be blocked. The only way to unblock the MMI would then be to modify the FFS file system.

4 Simulation Tests

The following simulation test cases will be added:

-Testcase 1. Get Security code state
%SECS?
%SECS: 1

-Testcase 2. Modify security code state
%SECS=0, ”12345”
OK,+CME ERROR

-Testcase 3. Verify security code
%SECP=”12345”
OK,+CME ERROR

-Testcase 4. Change security code
%SECP=”12345”, ”54321”
OK,+CME ERROR

Testcase 5. Set security code /* Not Implemented at the moment */
%SECP=, ”54321”
OK,+CME ERROR

Similar functionality will be tested in the target.