



Qisda Subsidy Lock Wizard

Document Number:

Version: 0.1

Date: 2008/05/27

Author:

Approval:

Document Revision History

Version	Date	Author	Comments
0.1	2008/05/27		



Content

1	Introduction	6
1.1	Purpose	6
1.2	Scope	6
1.3	Abbreviation	6
2	General Description	7
2.1	The Purpose of Subsidy Lock	7
2.2	Type of Subsidy Lock	7
2.2.1	Network Lock	7
2.2.2	Network Subset Lock	7
2.2.3	Service Provider Lock	8
2.2.4	Corporate Lock	8
2.2.5	SIM Lock	8
2.3	Prepare Lock	8
3	How to Use Subsidy Lock Wizard	9
3.1	Overview	9
3.2	Create Simlock File	9
3.2.1	Retry Setting	10
3.2.2	Global Setting	10
3.3	Lock Configuration	11
3.3.1	Network Lock	11
3.3.2	Network Subset Lock	11
3.3.3	Service Provider Lock	12
3.3.4	Corporate Lock	12
3.3.5	SIM Lock	13

Figures

Figure 3-1 Create new Simlock file.....9

Figure 3-2 Global setting detail..... 10

Figure 3-3 Global setting..... 10

Figure 3-4 Network lock setting..... 11

Figure 3-5 Network subset lock setting 12

Figure 3-6 Service provider lock setting..... 12

Figure 3-7 Corporate lock setting..... 13

This confidential document is the property of Qisda Corporation and must not be copied or circulated without permission.



References

Ref.	Document
<i>Standard</i>	
[1]	ETSI TS 101 624 (GSM 02.22) V7.0.0 Personalisation of GSM Mobile Equipment

1 Introduction

1.1 Purpose

The main purpose of the document is to give a description of subsidy lock wizard. Subsidy lock wizard is a tool helping user to edit variant subsidy lock configurations. The tool does not have the ability to encrypt/decrypt, so addition tool, called subsidy lock encoder, is needed when writing this subsidy lock configuration to UE.

1.2 Scope

The scope of the document is usage of subsidy lock wizard, and basic concept of personalization defined in [1]. How to encrypt/decrypt subsidy lock data, verify procedure in UE, however, are not in the scope of this document.

1.3 Abbreviation

For the purpose of the present document, the following abbreviations apply:

- DCK Depersonalization Control Key
- EF Elementary File
- GID1 Group Identifier (level 1)
- GID2 Group Identifier (level 2)
- IMSI International Mobile Subscriber Identify
- MCC Mobile Country Code
- MNC Mobile Network Code
- MSIN Mobile Subscriber Identification Number
- UE User Equipment

2 General Description

2.1 The Purpose of Subsidy Lock

The purpose of subsidy lock is to protection the subsidies from operators. Sometimes, operator subsidizes customers in UE price to let them use high price UE but pay low. For operator, it wants its users use the subsidized UE in its network at least a span of few years, or this investment will not gain proper return. So, the functionality of subsidy lock is to limit the UE to use the specific card. Specific card in subsidy lock means the card has specific values in certain EFs, including EF_{IMSI}, EF_{GID1}, and EF_{GID2}. A subsidy lock contains the limitation of these EFs.

After few years, operator might want to permanent disable subsidy lock for marketing or contract. It provides user a DCK to disable the subsidy lock. At this time, user frees to use the UE with any card.

2.2 Type of Subsidy Lock

The type of subsidy lock is defined in [1] as personalization. In the specification, there are 5 type of personalization. In the following content, the document use lock as personalization.

2.2.1 Network Lock

Network lock limits the MCC/MNC of card, which is part of IMSI (1~5 digits, or 1~6 digits). Every operator has different MCC/MNC, so this is the most common type of subsidy lock.

2.2.2 Network Subset Lock

Network subset lock limits the MCC/MNC, and up to 4 addition digits of IMSI. The addition digit can be any digit in MSIN, so subsidy lock wizard needs not only the limitation of digit, but which digit applied the limitation.

2.2.3 Service Provider Lock

Service provider lock limits the MCC/MNC, first and second octets of GID1 of card.

2.2.4 Corporate Lock

Corporate lock limits the MCC/MNC, first and second octets of GID1, first and second octets of GID2.

2.2.5 SIM Lock

SIM Lock limits all digits of IMSI of card, which means the UE can use the only card. Due to the nature of the lock, subsidy lock wizard only supports prepare lock of this type. The detail of prepare lock is in section 2.3.

2.3 Prepare Lock

Prepare lock is automation personalization defined in section 12 in [1]. UE with prepare lock will lock itself according to subsidy lock configuration and first card inserted. Because EF_{GID1} , and EF_{GID2} is optional in standard, prepare service provider lock and prepare corporate lock shall be avoided.

3 How to Use Subsidy Lock Wizard

3.1 Overview

Simlock wizard is divided in four main sections: The toolbar at the top of the window, the tree on the left side, the grid on the right side and the message list at the bottom.

The toolbar provides almost every function you need to create, edit or store simlock data.

The tree represents the current simlock file with its filename, the global file settings, its blocks with their block types and the locks. By double clicking you can edit the selected tree node. Selecting a lock in the tree will also select the corresponding data line in the grid.

In the grid you can see the lock data of the current simlock file. The columns represent "No.", "Mcc", "Mnc", "Gid1", and "Gid2".

3.2 Create Simlock File



Figure 3-1 Create new Simlock file

Use this dialog to select or type in a product and a provider for the new file you are about to create. Once a simlock file is created these setting cannot be changed. The product and provider information appear as part of the generated filename. After creating a new simlock file, double click on the Globalsetting in the tree on the left side, there is a dialog as the following figure,

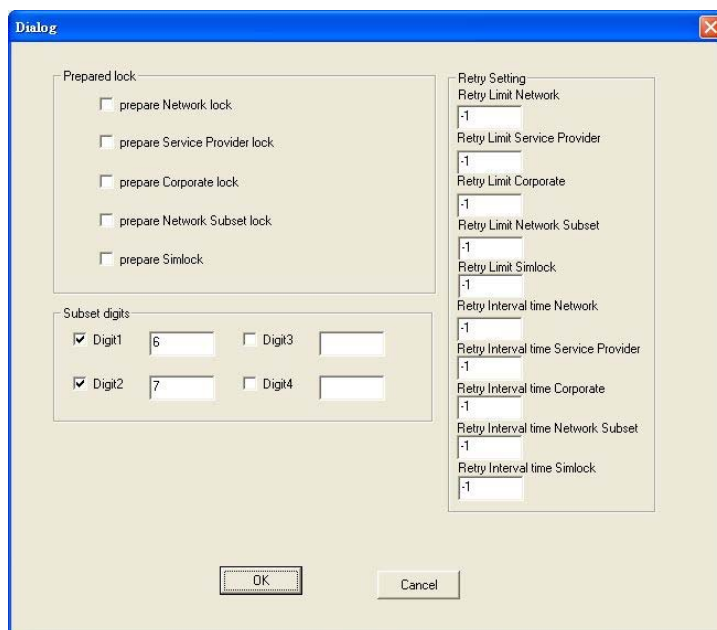


Figure 3-2 Global setting detail

3.2.1 Retry Setting

Retry setting is penalty setting when user provide a wrong DCK. Retry limit is the maximum attempt of single lock. When wrong DCK attempt exceeds retry limit, UE will be locked and cannot be unlocked. Retry interval is timing penalty, when user provide a wrong DCK, it cannot enter another DCK unless retry interval seconds pass. This two configurations increase the difficulty of brute force attack.

3.2.2 Global Setting

Once the global settings are specified, right click on Globalsetting in the tree on the left side and select New, there are four types of lock settings to chose, including Network lock, Network Subset lock, Service Provider lock, and Corporate lock.



Figure 3-3 Global setting

UE supported up to 25 sim lock configurations.

3.3 Lock Configuration

3.3.1 Network Lock

Specify the values "Mcc" and "Mnc". To use 3 digits instead of 2 digits for "Mnc" check "use 3 Mnc digits". Click on "Ok" to add or change a network lock.

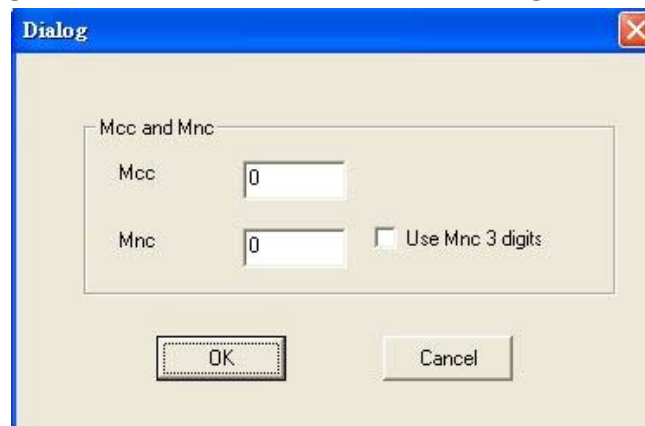
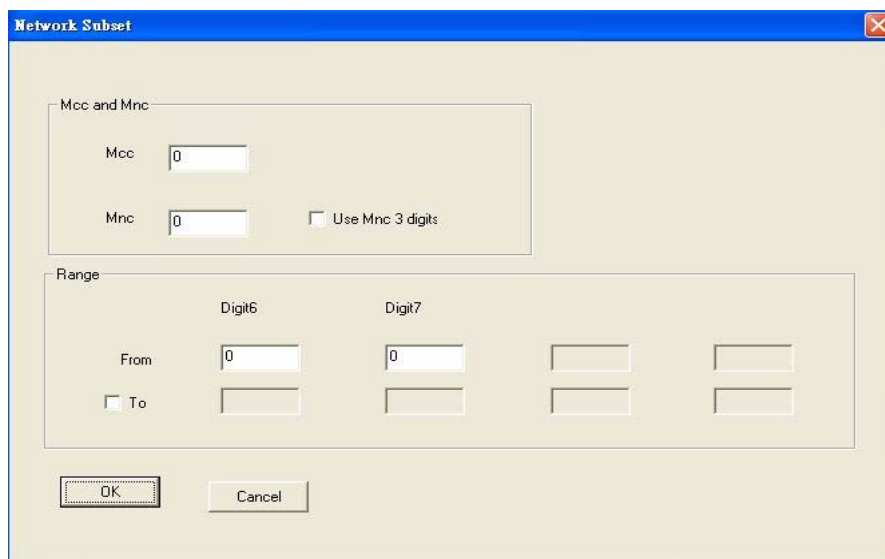


Figure 3-4 Network lock setting

3.3.2 Network Subset Lock

Specify the values "Mcc" and "Mnc". To use 3 digits instead of 2 digits for "Mnc" check "use 3 Mnc digits". The range for the specified digits must be set as well. Assign the digits you want to set by checking their checkboxes. If range start and range end are different for one or more digits you must check "to". To add or change the network subset lock click "Ok".



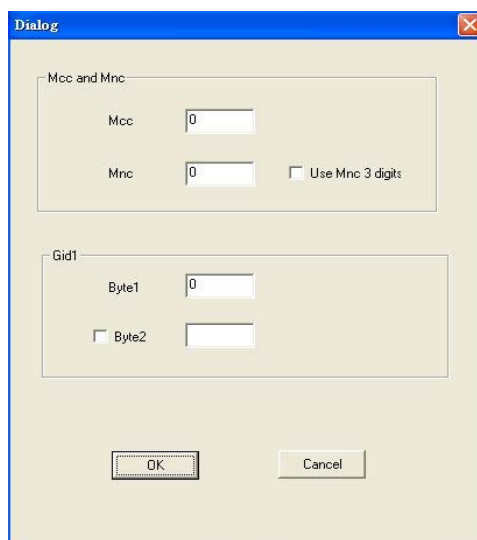
The 'Network Subset' dialog box contains two main sections. The 'Mcc and Mnc' section has input fields for 'Mcc' (value 0) and 'Mnc' (value 0), with an unchecked checkbox 'Use Mnc 3 digits'. The 'Range' section has a 'From' label and two input fields for 'Digit6' (value 0) and 'Digit7' (value 0), followed by two empty input fields. Below these is an unchecked checkbox 'To' followed by two more empty input fields. At the bottom are 'OK' and 'Cancel' buttons.

Figure 3-5 Network subset lock setting

3.3.3 Service Provider Lock

Specify the Values "Mcc" and "Mnc". To use 3 digits instead of 2 digits for "Mnc" check "use 3 Mnc digits". The "Gid 1" also has to be set. You can set this value either as decimal, hexadecimal or ASCII. You may assign the first, the second or both bytes of this Value.

To add or change the Service provider lock click "Ok".



The 'Dialog' box for service provider lock settings contains two main sections. The 'Mcc and Mnc' section has input fields for 'Mcc' (value 0) and 'Mnc' (value 0), with an unchecked checkbox 'Use Mnc 3 digits'. The 'Gid1' section has input fields for 'Byte1' (value 0) and 'Byte2' (empty), with an unchecked checkbox 'Byte2'. At the bottom are 'OK' and 'Cancel' buttons.

Figure 3-6 Service provider lock setting

3.3.4 Corporate Lock

Specify the Values "Mcc" and "Mnc". To use 3 digits instead of 2 digits for "Mnc"

check "use 3 Mnc digits". The "Gid 1" and the "Gid 2" also have to be set. You can set these values either as decimal, hexadecimal or ASCII. To add or change the corporate lock click "Ok".

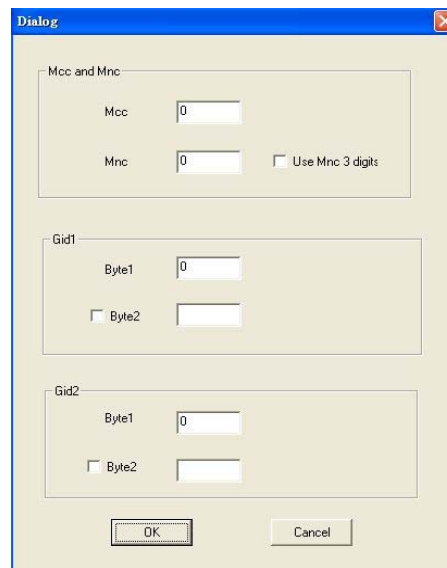


Figure 3-7 Corporate lock setting

3.3.5 SIM Lock

As mention before, SIM lock only supports prepare lock.