公務出國報告

(出國類別：實習)

第三代行動電話系統 USIM 技術實習報告

服務機關：中華電信行動通信分公司

出國人：　職　　稱：科長

姓　　名：胡學海、張明聰

出國地區：歐洲：芬蘭

出國期間：92.10.11 至 92.10.24

報告日期：92.12.30

報告人：張明聰、胡學海

系統識別號:C09204292

公 務 出 國 報 告 提 要

頁數: 42　含附件: 否

報告名稱:

實習「第三代行動電話系統USIM技術」

主辦機關:

中華電信行動通信分公司

聯絡人／電話:

陳月雪／(02)3316-6172

出國人員:

張明聰　中華電信行動通信分公司　網路維運處　科長
胡學海　中華電信行動通信分公司　加值處　科長

出國類別: 實習

出國地區: 芬蘭

出國期間: 民國 92 年 10 月 11 日 -民國 92 年 10 月 24 日

報告日期: 民國 92 年 12 月 30 日

分類號/目: H6／電信　H6／電信

關鍵詞: USIM,SIM,UICC

內容摘要: 雖然SIM(Subscriber Identity Module)卡只是GSM行動電話系統的一個小螺絲釘，但卻也是一個關鍵的系統元件，用戶端設備(UE)透過無線界面接取(Access)系統，藉由系統所提供的安全認證及加密機制，以及(U)SIM卡所儲存之個人身分認證資訊，提供了無線通訊的安全保障，隨著行動電話技術之演進，行動電話之服務重心已由語音(Voice)服務進入數據(Data)服務的時代，因此除了基本通信服務外，各類行動加值服務的開發預料將是未來行動通信服務提供者的服務重點，此種服務趨勢將更顯(U)SIM卡的重要性。本報告就USIM及其UICC卡片平台等相關技術及Gemplus 公司之OTA應用平台, ADE系統等提出個人實習心得。

本文電子檔已上傳至出國報告資訊網

附件二

出國報告摘要

出國報告名稱：第三代行動電話系統 USIM 技術實習報告

頁數__42__

含附件：□是■否

出國計畫主辦機關/連絡人/電話：

出國人員姓名/服務機關/單位/職稱/電話

張明聰/中華電信行動通信分公司/網維處/科長/02-33166596

胡學海/中華電信行動通信分公司/加值處/科長/02-33166488

出國類別：□1 考察□2 進修□3 研究■4 實習□5 其他

出國期間：92 年 10 月 11 日至 92 年 10 月 24 日　　出國地區:芬蘭

報告日期：92 年 12 月 30 日

分類號/目：交通/電信

關鍵詞：USIM, UICC, SIM

內容摘要：

雖然 SIM(Subscriber Identity Module)卡只是 GSM 行動電話系統的一個小螺絲釘，但卻也是一個關鍵的系統元件，用戶端設備(UE)透過無線界面接取(Access)系統，藉由系統所提供的安全認證及加密機制，以及(U)SIM 卡所儲存之個人身分認證資訊，提供了無線通訊的安全保障，

隨著行動電話技術之演進，行動電話之服務重心已由語音(Voice)服務進入數據(Data)服務的時代，因此除了基本通信服務外，各類行動加值服務的開發預料將是未來行動通信服務提供者的服務重點，此種服務趨勢將更顯(U)SIM 卡的重要性。

本報告就 USIM 及其 UICC 卡片平台等相關技術及 Gemplus 公司之 OTA 應用平台, ADE 系統等提出個人實習心得。

1. 目的

雖然 SIM(Subscriber Identity Module)卡只是 GSM 行動電話系統的一個小螺絲釘，但卻也是一個關鍵的系統元件，用戶端設備(UE)透過無線界面接取(Access)系統，藉由系統所提供的安全認證及加密機制，以及 SIM 卡所儲存之個人身分認證資訊，提供了無線通訊的安全保障，

隨著行動電話技術之演進，行動電話之服務重心已由語音(Voice)服務進入數據(Data)服務的時代，因此除了基本通信服務外，各類行動加值服務的開發預料將是未來行動通信服務提供者的服務重點。

爲支援未來多樣化的加值服務需求以及提供更安全的應用開發環境，3GPP 標準在 GSM 規範的 SIM 卡做了若干的增強，以配合此新一代的行動通信時代來臨。

本公司第三代行動電話系統乃是採用 3GPP 標準的 WCDMA 行動電話系統，USIM(Universal Subscriber Identity Module)爲此標準之用戶識別元件。本案實習之目的即在學習 USIM 技術，掌握最新資訊。

2. 過程

本實習案乃依據中華電信股份有限公司 92 年 10 月 2 日信人二字第 92A3501705 號函，赴本分公司行動電話系統合約案得標廠商 Nokia 公司實習【第三代行動電話系統 USIM 技術】。

實習過程以課堂講課爲主方式進行，由本案合約廠商 Nokia 公司安排專業講師就 USIM 架構，相關規範，系統安全環境等主題，另外搭配 OTA 的 ADE 應用環境實習等方式講解。

3. 心得

MS 爲 PLMN(Public Land Mobile Network)系統(參考圖 1)之用戶端實體元件，由 ME 及 SIM(R99 版本以後稱爲 USIM)組成，透過無線界面接取系統。

雖然 USIM 只是整個 PLMN 系統架構的一個應用程式模組，但是因爲其存放用戶個人身分認證資訊，也存放系統安全(Security)運作架構所需之各種安全資訊，加上 UICC 的 Multi application 應用環境等，故 USIM 應用程式模組架構以及相關安全環境等主題爲本報告之重點。

以下各節就本案 USIM 實習主題提出心得報告，

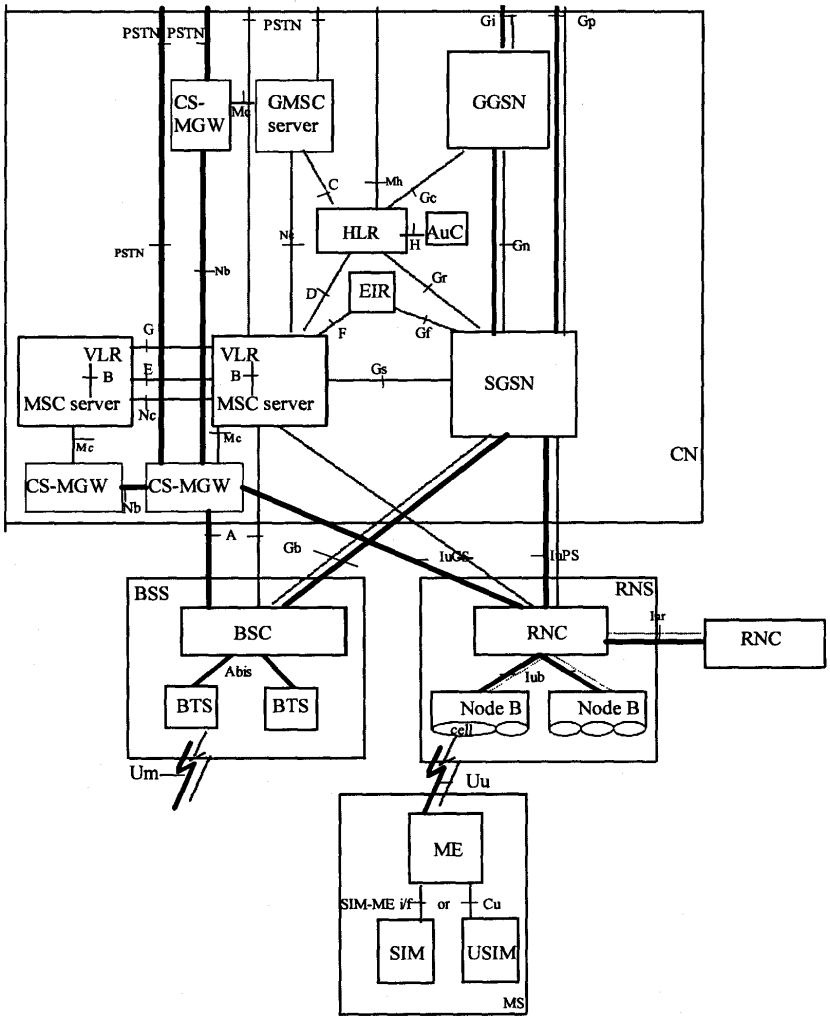


圖 1 ：Basic configuration of a PLMN supporting CS and PC serivices and interfaces

3.1 ICC、UICC、USIM、SIM

2G 行動電話系統由 GSM 演進到 3G 的 WCDMA 系統架構，用戶端設備的 SIM 卡規範也配合新技術及服務的需求而有所加強，雖然其主要作用仍然相同，

但是 3G 規範給了新架構 SIM 卡新的稱呼，爲免避混淆，本節首先針對幾個可能較易混淆的相關名詞稍作說明。

ICC(Integrated Circuit Card)爲一般 Smart card 的統稱.，而 UICC 卡則爲 3G 規範所制定，用以搭配 ME 設備存取 3G 系統服務之 ICC 卡；SIM 卡則是 2G 規範所制定，用以搭配 ME 設備存取 2G 系統服務之 ICC 卡。

UICC 卡的 Universal 意旨 UICC 卡可以共存多個 application，除了存取 3G 系統的 USIM application 外，也可以建立其他加值應用程式，如行動銀行，行動商務應用程式等。

SIM 卡爲單一應用程式之卡片，是一個同時規範 Physical 及 Logical 特性的實體(entity)。

3.2 Specifications

構成 USIM 及其卡片實體平台 UICC 之主要規範如下：

(A) Card physical and logical related specifications
- 3G TS 31.101 : UICC-Terminal Interface; Physical and Logical Characteristics
- 3G TS 31.102 : Characteristics of USIM application
- 3G TS 31.111 : USIM Application Toolkit(USAT)

(B) Security algorithms related specifications
- 3G TS 33.102 :Security Architecture
- 3G TS 33.105 - Cryptographic Algorithm Requirement
- 3G TS 35.206 – Specification of Milenage algorithm
- 3G TS 35.205 – Specification of Milenage algorithm

(C) OTA related specifications
- 3G TS 23.048 Security Mechanisms for the (U)SIM application toolkit
- 3G TS 23.040 Technical realization of the Short Message Services(SMS)

3.3 UICC

3GPP TS 31.101 規範 UICC 卡片平台之實體及邏輯特性，與 ME 設備組成 3G 系統之 MS 元件，其主要規範內容如下：

(A) UICC卡實體特性
(B) UICC卡界面電氣特性
(C) 傳輸協定
(D) 指令及程序

(E) 檔案架構與協定

UICC 卡之多應用程式支援架構，除可同時存在多個 UISM 應用程式外，也可以同時存在諸如 Banking 等之應用程式，其卡片之邏輯示意如圖 2 所示。

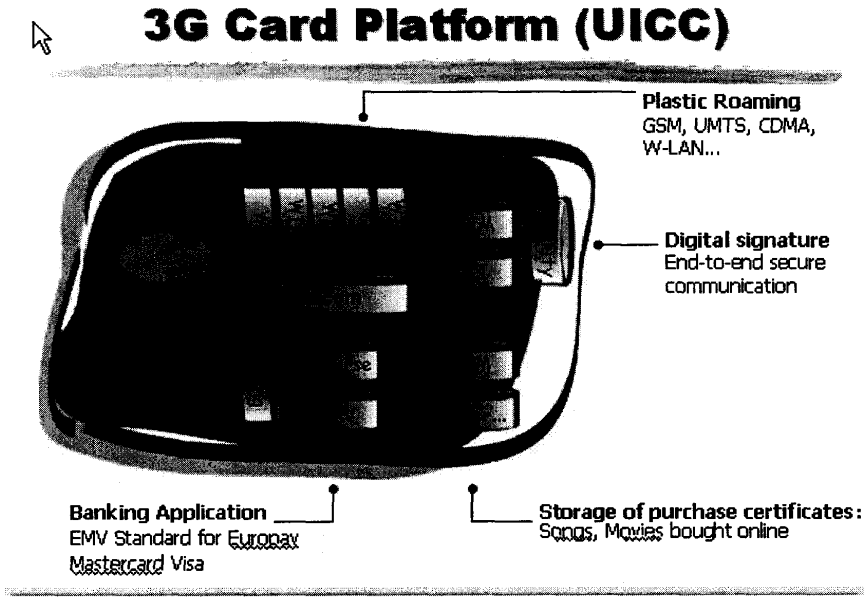


圖 2：UICC 架構邏輯示意圖

3.3.1 Physical, Electrical Characteristics

UICC 卡之 Physical 特性乃依據 ISO/IEC 7816-1 及 ISO/IEC 7816-2 規範，訂定 ID-1 UICC 及 Plug-in UICC 兩種尺寸規格。

UICC 與 ME 界面的 Electrical 特性則依據 ISO/IEC 7816-3 規範，訂定有支援 5V, 3V 及 1.8V 三種工作電壓等級之卡片。

行動電話手機開機後，ME 首先以最低工作電壓提供 UICC，透過檢測是否收到 UICC 的 ATR 回應，ME 設備得以配合切換適當之工作電壓。

3.3.2 傳輸協定

由於 UICC 與 ME 的信號傳輸共用一個實體傳輸路徑(ICC 六個接點的其中一點)，規範並未設計多工工作模式，所以雙方之傳輸只能以 half-duplex 的方式執行。其傳輸協定之 Protocol stack 如下圖 3 所示。

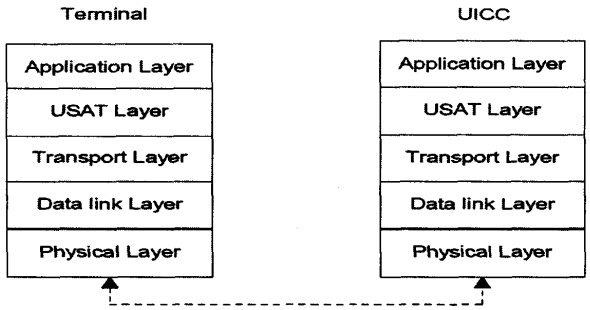


圖 3：UICC I/O protocol layers

UICC 支援 T=0 及 T=1 兩種模式的傳輸協定。T=0 模式傳輸協定爲 half-duplex 非同步 Character based 的協定；T=1 模式傳輸協定爲 half-duplex 非同步 Block bassed 的協定。

T=1 與 T=0 兩種傳輸協定的主要差異是，T=1 協定可以多點傳送，也多了錯誤檢查機制，所以兩者各有不同的適用範圍。以一般 ME 與 UICC 配合之應用而言，只需使用 T=0 模式傳輸協定。

ME 與 UICC 的協定交談以 Master-Slave 方式處理，ME 爲 Master 端，UICC 爲 Slave 端。Master 端發送命令，Slave 端則回應命令執行結果。由 ME 送往 UICC 之命令爲 Command-APDU，由 UICC 回應的命令爲 Response-APDU，兩種 APDU 合爲 APDU pair，其結構如表 1 及表 2。

表 1：Command APDU 結構

Mandatory header				Optional body		
CLA	INS	P1	P2	Lc	Data field	Le

表 2：Response APDU 結構

Optional body	Mandatory Trailer	
Data field	SW1	SW2

依據 Master 端的命令是否含有資訊以及是否要求 UICC 端傳回資訊，T=0 協定模式的 Transport 層交談的命令格式有下列四種情形。

表 3：Format of Command APDU

	Command APDU			
Case 1	Header			
Case 2	Header	Le		
Case 2	Header	Lc	Data	
Case 4	Header	Lc	Data	Le

Response APDU	
SW	
Data	SW
SW	
Data	SW

3.3.3 檔案架構與協定

整個 UICC 卡平台的檔案系統乃是由 MF 根目錄檔(目錄檔爲類似於一般電腦之目錄檔的群組檔案，此種群組檔案本報告均以目錄檔稱之)爲起始的階層式檔案架構，以及各應用程式之獨立階層式檔案組成。UICC 卡檔案系統範例架構詳圖 4。

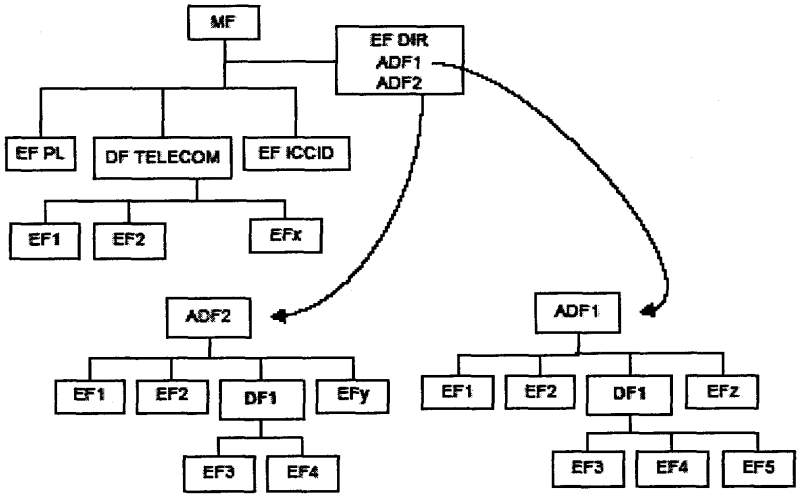


圖 4：Example of an application structure

所有的檔案依其特性可分爲 MF、EF、DF、 ADF 等四種。MF 檔案爲 UICC 檔案系統的根目錄檔案，其下可附掛 DF 及 EF 檔案；DF 爲一般性目錄檔案，其下可附掛其他的 DF 及 EF 檔案；而 EF 檔案爲一般性檔案，用以儲存用戶或應用程式資料。

ADF 爲特殊目的之目錄檔案，與其附掛之 DF 及 EF 檔案組成特定應用程式之階層檔案。UISM 及 GSM 應用程式即爲規範供 3G 及 2G 系統接取服務之應用程式，其 USIM 的 ADF 應用程式檔案架構另外規範於 TS 31.102 中。

EF 檔案之架構分 Transparent, Linear Fixed, Cyclic 等三種(如圖 5)，用以儲存不同性質之資料。

Transparent 檔案儲存是以 Byte 爲單位之連續性資料檔案，資料的存取以指定 Offset 位置及存取資料長度方式處理。

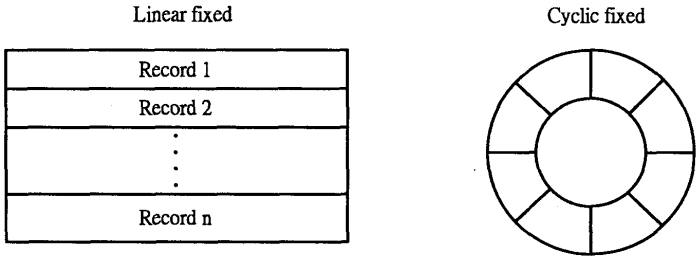


圖 5：EF file sturcture

Linear fixed 檔案儲存連續性，固定資料長度，以 Record 爲單位之資料檔案，資料的存取以 Record 爲單位。儲存資料時，檔案的 Record 指標隨指定方向移動到達盡頭時不再移動。

至於 Cyclic fixed 檔案儲存的也是連續性、固定資料長度，以 Record 爲單位之資料檔案，資料的存取也以 Record 爲單位，只是儲存資料時，檔案的 Record 指標隨指定方向移動到達盡頭時，record 指標繼續往前移動，並覆蓋掉該位置的資料。

在 MF 目錄檔下，EF_{DIR}, EF_{PL}, EF_{ICCID} 爲強制性檔案，$DF_{TELECOM}$ 檔案爲選擇性檔案。

各應用程式目錄檔，ADF1, ADF2...等，透過 EF_{DIR} 檔案指到相對應之應用程式。當 UICC 卡插入 ME，經過開機後之 ATR 程序後，UICC 卡自動選擇 MF 檔，隨後依據第一個 ADPU 指令的 Class 選擇 UISM 或是 GSM 應用程式。Class 爲"A0"時，選擇 GSM 應用程式，Class 爲"80"及"00"時，選擇 USIM 應用程式。(詳圖 6)。

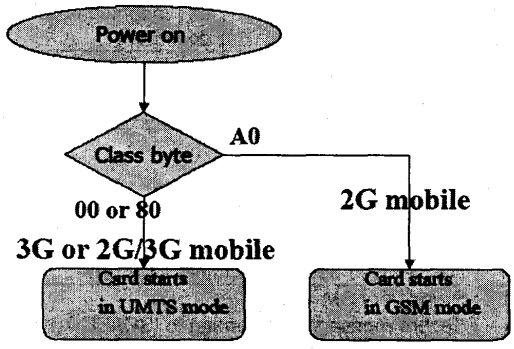


圖 6：USIM application selecture procedure

一般電腦由於具有強大的性能，作業系統也提供人性化的操控畫面，應用

程式可以透過方便的人機界面啓動，而一般的資料檔案則大多以單獨檔案方式儲存再由應用程式開啓。UICC 卡屬特定用途卡片，雖也具有 CPU，ROM，EEPROM，RAM，作業系統等電腦的主要軟、硬體零件，但其性能、特殊用途及架構均與一般電腦由極大差異，其應用程式與運作資料多已緊密結合，大多數應用程式運作資料也在卡片製作過程預爲載入，只要選取該應用程式 ADF 檔案，應用程式即啓動執行。

3.3.4 支援命令及格式

下列各節說明 Command 及 Response APDU 的細部規範。

3.3.4.1 Command APDU structure

表 4：APDU Command format

Code	Length	Description	Grouping
CLA	1	Class of instruction	Header
INS	1	Instruction code	
P1	1	Instruction parameter 1	
P2	1	Instruction parameter 2	
Lc 0	or 1	Number of bytes in the command data field	Body
Data	Lc	Command data string	
Le	0 or 1	Maximum number of data bytes expected in response of the command	

表 5：Coding of Class byt

B8	b7	b6	b5	b4	b3	B2	b1	Value	Meaning
0	0	0	0	-	-	-	-	'0X'	The coding is according to ISO/IEC 7816-4 [13]
1	0	1	0	-	-	-	-	'AX'	Coded as ISO/IEC 7816-4 [13] unless stated otherwise
1	0	0	0	-	-	-	-	'8X'	Structured as ISO/IEC 7816-4 [13], coding and meaning is defined in the present document
-	-	-	-	X	X	-	-	-	Secure Messaging indication (see table 10.4)
-	-	-	-	-	-	X	X	-	Logical channel number (see clause 10.3)

表 6：Coding of Security Messaging Indication

b4	b3	Meaning
0	0	No SM used between terminal and card
0	1	Proprietary SM format
1	x	Secure messaging according to ISO/IEC 7816-4 [13] used
1	0	Command header not authenticated
1	1	Command header authenticated

因爲 UICC 可以同時支援 2G SIM 以及 USIM 兩種應用程式，兩者的命令以不同的 Command Class 碼區別。SIM 的 Class byte 爲"Ax", USIM 的 Class byte 爲"0x" 及"8x"兩種。

UICC 在 ATR 的 Initial 或 Soft Reset 程序後，藉由第一個 Command 的 Class 碼判斷選用的 Application, 如果此 Class 碼爲"Ax"則選用 GSM 的 SIM Application；如果 Class 碼爲"0x"或"8x"則選用 USIM Application。Application 一經選定後，在整個 Application Session 程序中無法切換至其他的 Application 程序。

3.3.4.2 Coding of Instruction byte

下表爲 TS 31.101 制定之 Application Independent 命令及其 Class 與指令碼。

表 7：Command and Code table

COMMAND	CLA	INS
Command APDUs		
SELECT FILE	0X	'A4'
STATUS	8X	'F2'
READ BINARY	0X	'B0'
UPDATE BINARY	0X	'D6'
READ RECORD	0X	'B2'
UPDATE RECORD	0X	'DC'
SEARCH RECORD	0X	'A2'
INCREASE	8X	'32'
VERIFY	0X	'20'
CHANGE PIN	0X	'24'
DISABLE PIN	0X	'26'
ENABLE PIN	0X	'28'
UNBLOCK PIN	0X	'2C'
DEACTIVATE FILE	0X	'04'
ACTIVATE FILE	0X	'44'
AUTHENTICATE	0X	'88'
GET CHALLENGE	0X	'84'
TERMINAL PROFILE	80	'10'
ENVELOPE	80	'C2'
FETCH	80	'12'
TERMINAL RESPONSE	80	'14'
MANAGE CHANNEL	0X	'70'
Transmission oriented APDUs		
GET RESPONSE	0X	'C0'

3.3.4.3 Response APDU structure

下表爲由 UICC 回應 Command APDU 處理結果的 APDU 格式，表中的 Data 欄位是否實際送出視 Command 處理的結果而定。

表 8：Response APDU format

Code	Length	Description
Data	Lr	Response data string
SW1	1	Status byte 1
SW2	1	Status byte 2

3.3.5 安全機制

UICC 卡之安全機制乃依據 ISO/IEC 7816-9 標準，在每個檔案的的 FCP 控制參數表的'8B', '8C'或是'AB'三個欄位指定其安全屬性。

依據該規範，UICC 內部資源的安全屬性可以有 Compact format、Expanded format 以及 Access rule referencing 三種方式。物件安全屬性設定到底採用哪一種設定格式，基本上是視安全屬性設定的複查度而定。

安全屬性乃是由 Access mode 及 Security condition 兩個設定參數成對組合而成，Access mode 參數設定對該檔案的可執行動作，如 Read, Write, Delete 等，不同 UICC 卡資源的 Access mode 可能不同；Security condition 則設定執行該動作(Access mode 所設定的動作)所需的條件，如是否需要密碼的認證等。

下列表 9, 10 及 11 分別爲三種 Security attribute 之格式範例。

表 9：Compact format of security attribute

Tag	L	AM	SC	SC
'8C'	'03'	'03'	'10'	'00'

表 10：Expanded format of security attribute

Tag	L	AM_DO tag	AM_DO	SC_DO tag	SC_DO	AM_DO tag	AM_DO	SC_DO tag	SC_DO
'AB'		See ISO/IEC 7816-9		See ISO/IEC 7816-9		See ISO/IEC 7816-9		See ISO/IEC 7816-9	

表 11：EF_{ARR} Attribute referencing file format example

Record number(ARR)	Record content(Access rule)
'01'	AM_DO || SC_DO1 || SC_DO2 || AM_DO || SC_DO3 || SC_DO4...
'02'	AM_DO || SC_DO1 || AM_DO || SC_DO5 || SC_DO6...

FCP tag='8B' L='03' value='File id of EF_{ARR}, record number

3.4 USIM

USIM 爲 3G UICC 卡片平台上之應用程式規範，透過 USIM 應用程式，UICC 卡片得以插入任何廠牌手機，正常接取 3G 系統服務。

爲配合接取 3G 系統服務，USIM 應用程式除了必須執行 TS 31.101 UICC 規範所訂相關指令以及 USAT 指令外，也定義了接取服務有關的資料 Profile。

USIM 應用程式所有相關的資料存在於 UICC 的 MF 根目錄下的 UISM ADF 目錄，以下各節簡略說明各相關規範。

3.4.1 USIM Profile

USIM 所存放資料約可歸類爲下列幾種：

(A) 用戶身分識別資訊：
- IMSI。

(B) 服務設定資訊
- Service Table
- Cell broadcast related information
- Short message and related parameters
- Emergency call code

(C) 用戶認證及存取權限相關資訊：
- PIN, ADM 等密碼
- ARR

(D) 網路認證相關資訊：
- K, Ki, Kc, OPc, c1-c5, r1-r5。

(E) 網路接取相關資訊：
- Capability and Configuration parameters
- HPLMN search period
- BCCH information: list of carrier frequency to be used for cell selection

(F) OTA相關資訊
- 各項安全傳輸加密密碼等資訊

(G) 其他服務設定資訊：
- SMS configuration parameters
- Forbidden PLMN

(H) 用戶資訊：
- 電話簿
- 簡訊收發記錄
- 發/受話記錄

3.4.2 Phonebook

相較於舊版本的電話簿之功能，USIM 電話簿功能已做大幅修改，下列各項爲其主要修訂功能：

(A) 多組電話：此功能可允許一個人可設定多個電話號碼，

(B) 第二名稱：此功能允許給予第二個名稱，如匿名等。

(C) 群組功能：此功能可將公司電話或是私人電話分群管理。

(D) 傳真號碼：除了一般電話號碼外，傳真，E-mail 及公司網址等資訊都可以輸入。

(E) E-Mail 地址

(F) 網站地址

(G) 電話不容量大量擴充：如果USIM記憶容量足夠的話，電話簿容量可大幅擴充至65000筆。

(H) 多組電話簿功能：如果UICC卡容量許可的話，UICC內各應用程式可以允許建立各自的電話簿。

(I) 電話簿同步功能：此功能可提供使用者方便的電話簿管理功能，使UISM電話簿可與方便的與外部電話簿進行同步。

爲支援前述新增的電話簿功能，電話簿資訊必須由多個檔案共同組合而成(相關 EF 檔詳表 12)。所有 Phone book 使用到的 EF 檔案必須先在 EF_{PBR} 中宣告，同時指定與主檔案 EF_{ADN} 的對應關係。這些使用到的 EF 檔案與電話簿的主檔案資料的對應關係有三種，可以是一對一對應方式，也可以是透過 EF_{IAP} 進行連結的對應方式，也可以是直接以 Record Identifier 連結的方式。當電話簿容量超過每個 EF 檔最大 254 個 Record 筆數限制時，可以在 EF_{PBR} 中增列宣告以進行擴增。前述各項有關電話簿容量的規劃均必須在卡片製作過程中預先規劃。

圖 7 爲電話簿結構範例圖。本例電話簿大於 254 筆容量，所以需要由兩個 EF_{ADN} 檔案帶領相關的的 EF 檔；每筆電話可以有 4 組號碼，第二名稱，Email 位址，每筆資料可設定是否隱藏，也有群組功能，

表 12：EF files for phonebook

File name	Type 1	Type 2	Type 3	
EF_{PBR}				Phone book reference file
EF_{AAS}			X	Additional number Alpha String
EF_{ADN}	X			Abbreviated dialing number
EF_{ANR}	X	X		Additional number
EF_{EMAIL}	X	X		Email address
EF_{EXT1}			X	
EF_{GAS}			X	Grouping information alpha string
EF_{GRP}	X			Grouping file
EF_{IAP}	X			Index administration phone book
EF_{PBC}	X			Phone book control
EF_{SNE}	X	X		Second Name Entry
EF_{UID}	X			Unique Identifier

3.4.3 Security feature

爲接取系統，支援系統相關的安全機制，USIM 必須配合提供網路認證及加密等功能，此部份另於 3.6 節說明。

3.5 USAT

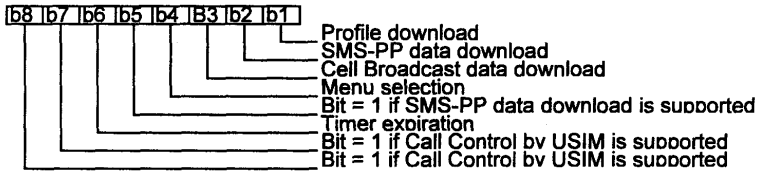
USAT 爲 TS 31.111 所規範所定義，提供 USIM Application 與 ME 運作有關之指令及程序，以控制手機螢幕與按鍵．USAT的設計使UISM得以控制手機的運作，開發 Handset-Independent 之應用程式．

3.5.1 Profile Download

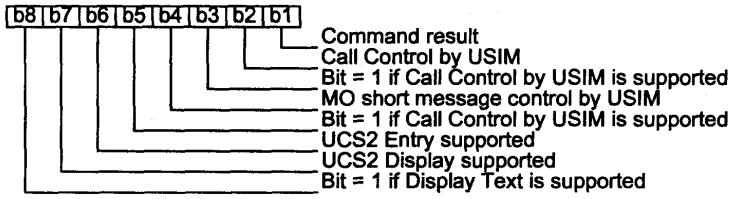
爲提供五花八門手機與 USIM 可以順利的溝通，Profile Download 機制允許ME設備將其可支援USAT能力的Profile資訊下載給USIM應用程式，使USIM可以配合手機功能調整互動行爲．

規範所定義之 ME 的 Profile 資訊如下：

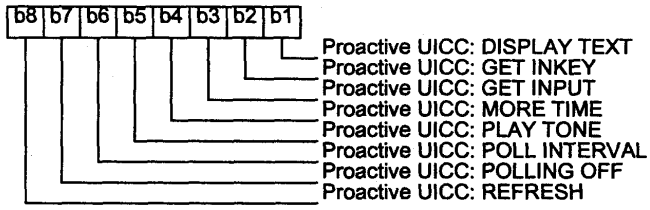
First byte (Download):



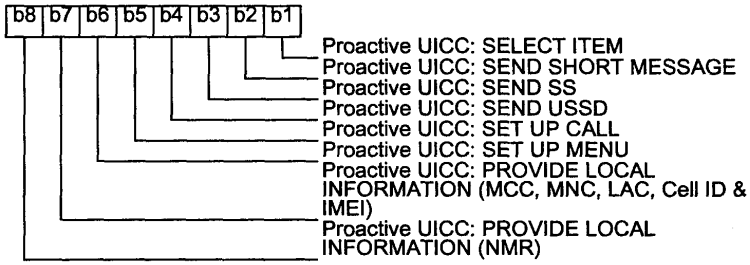
Second byte (Other):



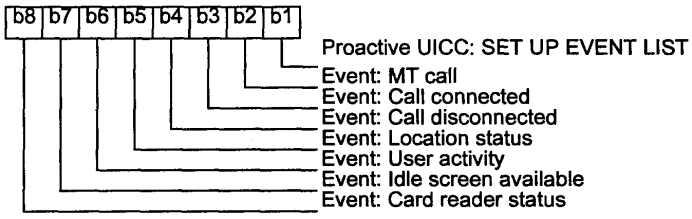
Third byte (Proactive UICC):



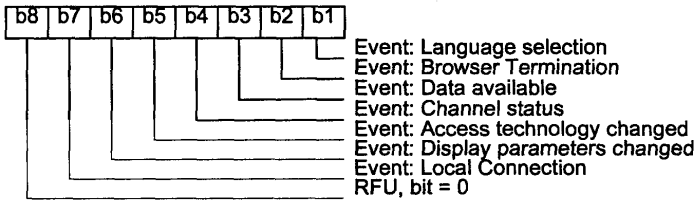
Fourth byte (Proactive UICC):



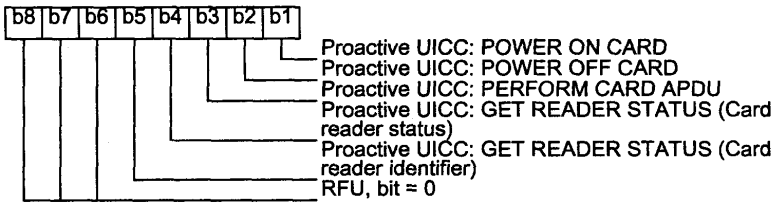
Fifth byte (Event driven information):



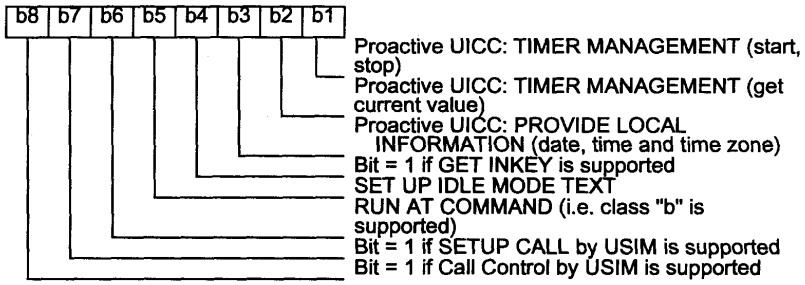
Sixth byte (Event driven information extensions):



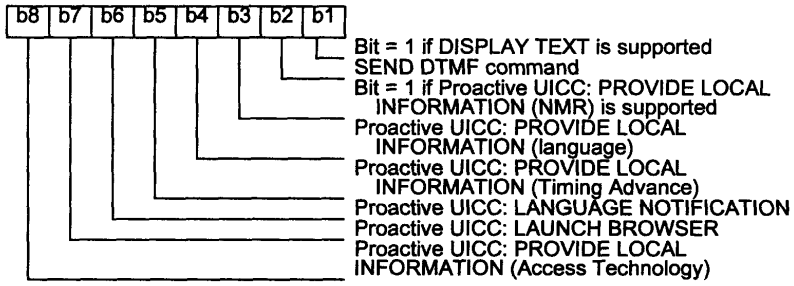
Seventh byte (Multiple card proactive commands) for class "a"



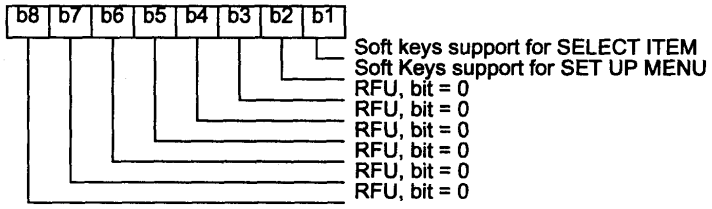
Eighth byte (Proactive UICC):



Ninth byte:

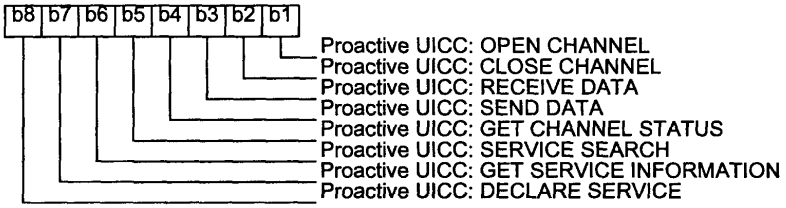


Tenth byte (Soft keys support) for class "d":

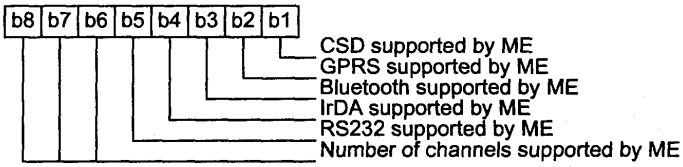


Eleventh byte: (Soft keys information)

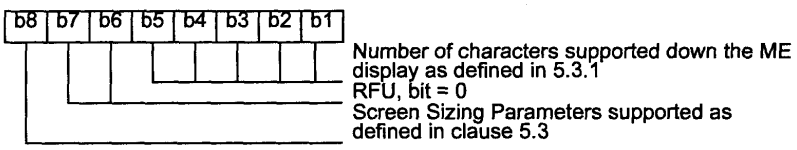
Twelfth byte:



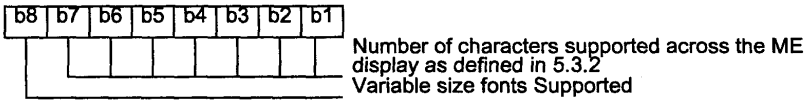
Thirteenth byte:



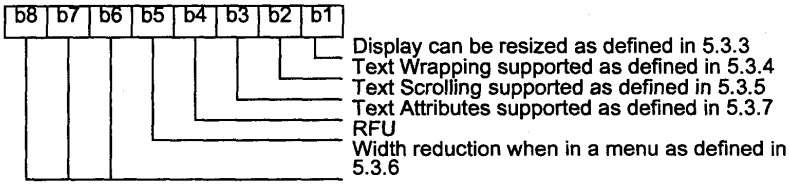
Fourteenth byte: (Screen height)



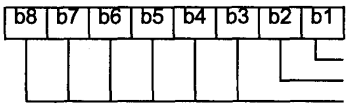
Fifteenth byte: (Screen width)



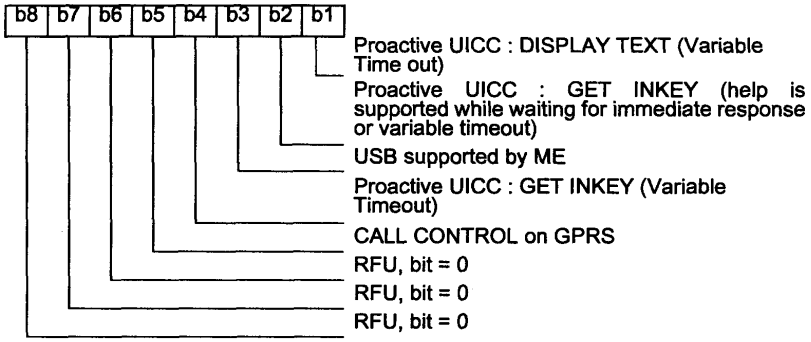
Sixteenth byte: (Screen effects)



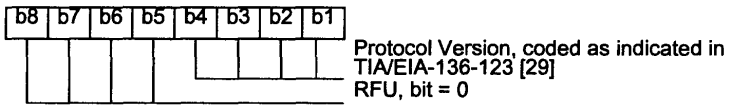
Seventeenth byte:



Eighteenth byte:



Nineteenth byte: (reserved for TIA/EIA-136 facilities):



3.5.2 Proactive UICC

ME 與 UICC 之間之通信協定爲半雙工(Half Duplex)模式，兩者以 Master-Slave 的方式進行溝通·ME 以 Master 角色對 UICC 下達命令，而 UICC 以 Slave 角色回應處理結果·如此的設計缺少了 UICC 主動送出命令的給 ME，而由 ME 回應處理結果的機制·

Proactive command 的設計提供模擬 UICC 主動送出命令給 ME，而由 ME 回送處理結果的機制·

此種模擬 UICC 主動送出命令給 ME 的方式是，在 UICC 正常完成 ME 命令時，以"91 xx"特定的回應碼(Status word)替代"90 00"正常回應碼，除了回應 UICC 正常完成 ME 命另外，也同時通知 ME 設備 UICC 有命令等待 ME 取回執行，ME 設備收到此訊息後，再以 Fetch 命令由 UICC 取回等待執行的命令，然後在命令成功執行完畢後，以 Response 命令將執行結果回送給 UICC·

特定回應碼"91 xx"的第二 Byte("xx")即是 Proactive command 的命令代碼·

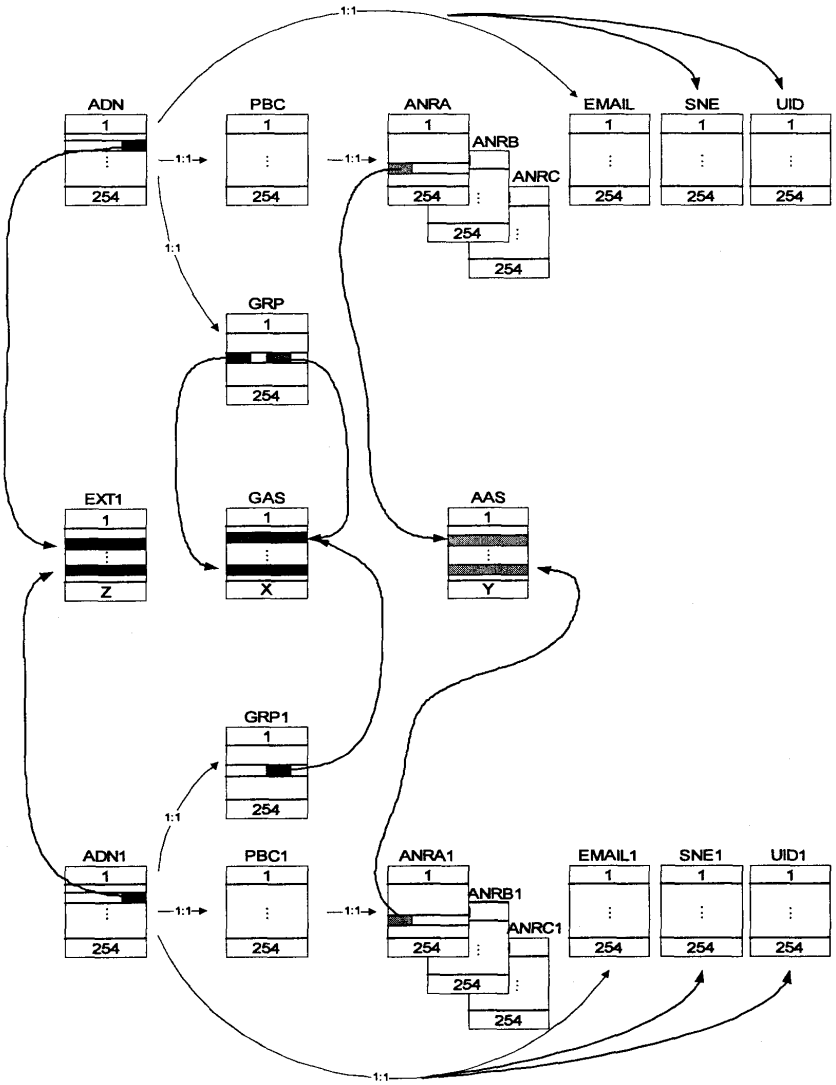


圖 7 ：Example of a Phonebook

Proactive Command 代碼及名稱如表 13 所示·

表 13：Proactive command list

Value	Name
'01'	REFRESH
'02'	MORE TIME
'03'	POLL INTERVAL
'04'	POLLING OFF
'05'	SET UP EVENT LIST
'10'	SET UP CALL
'11'	SEND SS
'12'	SEND USSD
'13'	SEND SHORT MESSAGE
'14'	SEND DTMF
'15'	LAUNCH BROWSER
'20'	PLAY TONE
'21'	DISPLAY TEXT
'22'	GET INKEY
'23'	GET INPUT
'24'	SELECT ITEM
'25'	SET UP MENU
'26'	PROVIDE LOCAL INFORMATION
'27'	TIMER MANAGEMENT
'28'	SET UP IDLE MODEL TEXT
'30'	PERFORM CARD APDU
'31'	POWER ON CARD
'32'	POWER OFF CARD
'33'	GET READER STATUS
'34'	RUN AT COMMAND
'35'	LANGUAGE NOTIFICATION
'40'	OPEN CHANNEL
'41'	CLOSE CHANNEL
'42'	RECEIVE DATA
'43'	SEND DATA
'44'	GET CHANNEL STATUS
'45'	SERVICE SEARCH
'46'	GET SERVICE INFORMATION
'47'	DECLARE SERVICE

3.5.3 Data Download to UICC

下列兩種信息途徑提供下載資料至 UICC 的機制，兩種命令信息以 UICC Envelope 命令包裝後,由 ME 直接送交 UICC 處理。

- SMS point-to-point or Cell broadcast
- Bearer independent protocol

3.5.4 Menu Selection

UICC 透過"Set up menu" Proactive command 提供選單給 ME，而此機制則將 user 在 ME 的選擇結果送給 UICC，以提供 USIM 應用程式進一步處理的資訊。

3.5.5 Call Control by USIM

如果 ME 設備支援此項機制的功能已被 USIM 啓動，則往後用戶撥叫電話或傳送 USSD 資訊時，用戶撥叫的資訊均會隨同用戶所在 Cell 資訊先傳送給 USIM 應用程式，以供 USIM 做特殊處理後再進行真正的撥叫動作。

3.5.6 MO Short Message control by USIM

與 Call control by USIM 機制相同的作用，ME 設備支援此項機制的功能如果已被 USIM 啓動，則往後用戶發送簡訊時，發送資訊會隨同用戶所在 Cell 資訊先傳送給 USIM 應用程式，以供 USIM 做特殊處理後再進行真正的發送動作。

3.5.7 Event Download

此項機制搭配"Set up event list" Proactive command，將 ME 的狀態資訊回傳給 USIM。"Set up event list" 命令設定 ME 狀態監視項目，而 ME 的狀態資訊則利用 UICC 的 Envelope 命令傳送給 USIM 應用程式。

ME 可監視的狀態資訊如下：

Event
MT call
Call connected
Call disconnected
Location status
User activity
Idle screen available
Card reader status
Language selection
Data available
Channel status
Browser termination
Access technology changed
Display parameters changed
Local connection

3.5.8 Multiple card

此項機制提供 ME 介接多 UICC 卡的功能，而這些 UICC 卡分別執行不同的應用程式。

3.5.9 Timer Expiration

此項機制允許 UICC 利用 ME 所提供的 Timer 功能，以供應用程式使用。

3.5.10 Bearer Independent Protocol

此項機制結合"Open channel"，"Close channel"，"Send data"，"Receive data" and "get channel status" 等 Proactive command，以及 "Data

available", "Channel status"等 Event download 命令，使 UICC 可以透過 ME 與遠端的伺服器建立資料傳輸通道

3.6 Security of UISM

有關 USIM 的 Security 問題，涉及 MS 與系統網路的認證，用戶的認證以及通信資訊如何加密等項目。

在用戶的認證方面，使用者必須輸入所謂的 PIN 密才可以開啓手機，依據不同 PIN 的權限等級，UISM 會給予不同程式或檔案等 UICC 卡內部資源的存取權限。

至於 MS 與系統端的網路認證與資料加密的密碼協商程序就是所謂的 Algorithm and Key Agreement(AKA)程序。

3G 規範之 AKA 機制採 Milenage 認證架構，與 2G 規範的認證架構相較，有如下之新的功能：

(A) 雙向認證機制：

過去 2G 系統的認證架構只有 User 端認證，新架構的 AUTN 設計增加了雙向認證機制。HLR/AuC 藉由 AUTN 送出其身分資訊給 UISM，USIM 則藉由送回正確的 RES 證明本身之身分。

(B) Signalling加密

在 Radio access interface 除了 DATA 加密外，新架構也對 Signalling 加密，以提高多一層的保障。

(C) 彈性認證法則機制

Milenage 認證架構的 AMF 設計預留多運算法則的機制，系統與 USIM 可可經由協調變更 Milenage 機制採用的運算法則。此項設計可提高 AKA 程序的安全性。

(D) 差異化認證機制

藉由選擇不同的 OP 碼以及 c1-c5, r1-r5 等 Milenage 認證架構參數，不同系統雖然採用共同的認證機制，卻可有差異化的結果。此架構也增加了認證系統的安全性。

3.6.1 相關網路元件參數及 algorithm

爲完成安全認證及加/解密作業，相關網路元件必須具備之參數或是 Algorithm 如下：

(E) UISM

- K, OP (per subscriber)
- IMSI (per subscriber)
- Milenage algorithm

(F) ME

- f8, f9 algorithm（KASUMI）

(G) RNC

- f8, f9 algorithm (KASUMI)

(H) HLR/AuC

- IMSI (per subscriber)
- K, OP (per subscriber)
- Milenage algorithm

網路之 AKA 程序在 HLR/AuC 及 USIM 之間執行。加密作業則在 RNC 及 ME 間執行。

3.6.2 The Milenage algorithm

Milenage algorithm 用以產生 f1, f1*, f2, f3, f4, f5, f5* 等認證需要有關之函數，其架構如圖 8 說明。

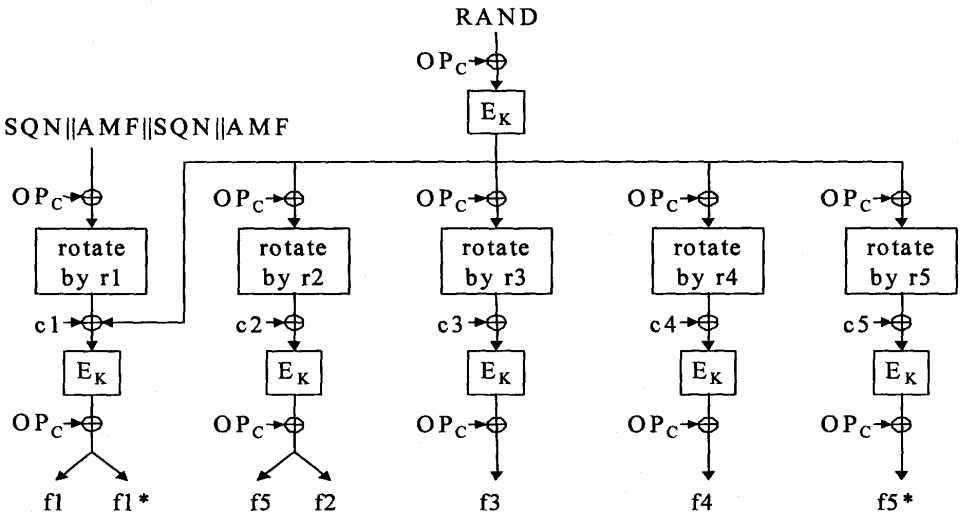


圖 8：Milenage algorithm structure

3.6.3 系統元件配合功能

參與網路認證程序之網路元件主要有 HLR/AuC,及 USIM，各元件須配合的機制說明於後。

3.6.3.1 Generation of quintets in HLR/AuC

HRL 收到認證請求後，依下圖機制計算 MAC-A, XRES, CK, IK 等參數，進而組合相關資料產生 AUTN。圖中的 RAND 採用 f0 函數產生。

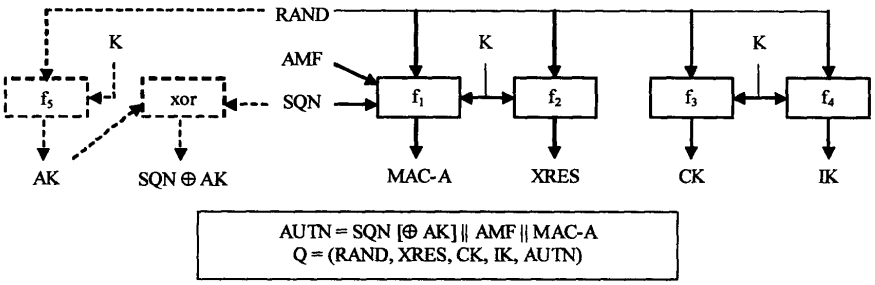


圖 9：Generation of quintets in the AuC

3.6.3.2 Authentication and Key derivation in USIM

USIM 收到(RAND, AUTN)後，依下圖機制還原 SQN，也同時確認 HLR/AuC 之身分，並進而計算 XMA-C, RES, CK 以及 IK。

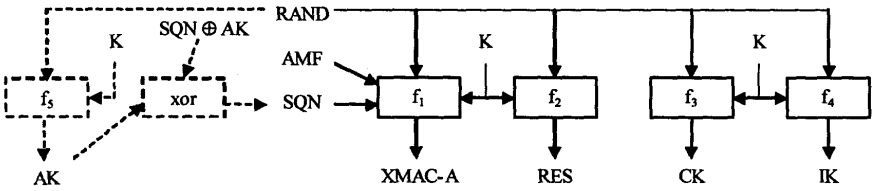


圖 10：Authenticatin and key derivation in the USIM

3.6.3.3 Generation of re-synchronisation in the USIM

USIM 確認收到錯誤的認證參數後，依下圖產生 re-synchronization token, AUTS。

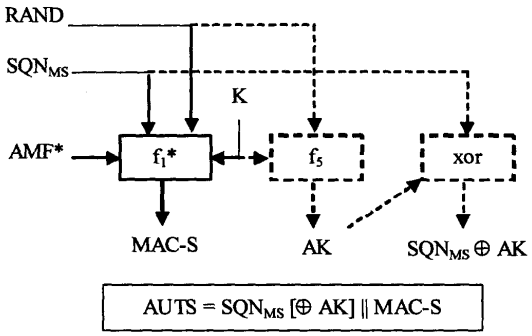


圖 11：Generation of re-synchronization token in the USIM

3.6.3.4 Re-syncrhonisation in the HLR/AuC

收到 USIM 回送的(AUTS, RAND)後，HLR/AuC 依下圖執行解碼，並比對 MAC-S 與 XMAC-S。

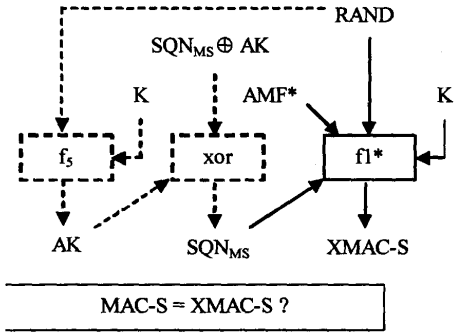


圖 12：Re-synchronization in the HLR/AuC

3.6.4 網路認證程序

整個 Authentication and Key Agreement 之程序如下圖所示。

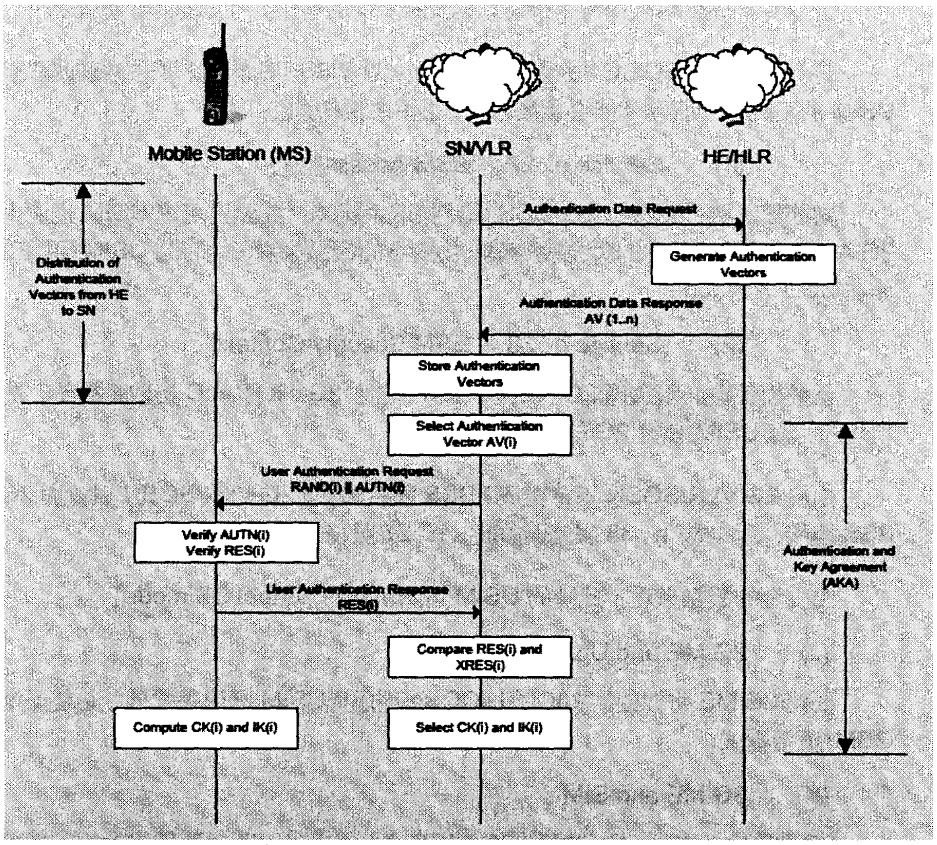


圖 13：Authentication and key agreement procedure

3.7 Interworking between the ME and the UICC

3G 行動電話系統乃由 2G 系統逐漸演進，系統設計時已考量兩代系統間的 IOT 機制；另外，在 User 端的 MS 也有同樣的設計，3G 的 UICC 卡以及 2G 的 SIM 卡都可以插入 2G 或 3G 手機使用。

由於有新、舊兩代系統並存，以及用戶端手機與卡片多樣化組合，以及系統業者營運政策的關係，展現的服務功能將因之而有所差異。

以下各節由不同的幾個主題說明可能的組合以及其現象或限制。

3.7.1 Interworking between the ME and the ICC

2G 與 3G 兩種 ME,以及 SIM 與 UICC 兩種卡片有下列四種可能的搭配使用方式：

(I) 3G ME and UICC

當 UICC 搭配 3G 單模手機時，只支援 3G 的命令，不支援 2G 的指令·

當 UICC 搭配 2G/3G 雙模手機時,如果要使 MS 可以接取 2G 的無線網路，USIM 的下列兩項服務功能必須開啓，以提供相關功能·

(1) Service n° 27："GSM Access"

當雙模手機必要透過 2G BSS 網路接取系統時，此設定可讓 USIM 也產生 2G Access 網路所需的 Kc 加密密碼·由安全的觀點來看，此時的 USIM 可謂工作在"3G + Kc mode"·

(2) Service n° 38："GSM Security Context"

當雙模手機必須透過 2G VLR/SGSN 或者 2G HLR/AuC 接取系統時，此項功能可讓 USIM 執行 2G 的 AKA 程序·

由於 2G VLR/SGSN 不會與 3G BSS 連接,意即 2G VLR/SGSN 只會與 2G BSS 連接，所以當 n° 38 服務開啓時，n° 27 服務也會同時開啓·

由安全的觀點來看，此時的 USIM 可謂工作在"Virtual 2G mode"·

(J) 2G ME and UICC

要使 2G ME 可以使用 UICC, UICC 除了提供 USIM 應用程式外，必須提供 GSM 應用程式·

(K) 3G ME and SIM

3G ME 由於支援 2G SIM 與 3G UICC 卡片的界面,所以此種組合的 MS 可以接取 2G 或 3G 系統·當然，接取 3G 系統時只能提供 GSM 類似的功能，而且也必須視 3G 系統業者的開放意願而定·

(L) 2G ME and SIM

此種組合的 MS 當然只能接取 2G 網路·

3.7.2 Authentication and Key agreement in mixed networks

MS 的網路 AKA 程序涉及 ICC, ME, ICC, BSS, VLR/SGSN 以及 HLR 網路元件，而這些元件又可能有 2G 與 3G 的差異，所以，所有網路元件的組合情況最多有 32 種·扣除某些不可能的組合情況，譬如，2G ME 不可能接取 3G BSS 元件，而以 ICC/ME 組合分類的理論可能組合情形如下四節說明·

(A) With 3G ME and UICC

本群組合情形總共應有 8 種，但是，因爲 Case 3 的 2G VLR/SGSN 無法與 3G BSS 搭配；Case 5 的 UICC/ME 只支援 3G 的 AKA 程序，與 2G 的 HLR/AuC 無法搭配；Case 7 的情形與 Case 3 相同，2G VLR/SGSN 無法與 3G

BSS 搭配。

其他的組合情形需要如開啓USIM的n° 27或是n° 38服務選項，啓動USIM的"3G + Kc Mode"或是"Virtual 2G mode"或是必須搭配 2G/3G 雙模 ME。

由於本分公司的 2G 網路與 3G 網路爲兩個獨立的網路，兩個網路間 HLR 以下各層元件不會有互連的情形，所以實際上在本網可能只會有 Case 1、Case 4 及 Case 8 的組合情形。但是，如果考慮用戶漫遊的情形，組合情況可能會比較多。

表 14：Possible Interworking scenarios of a 3G ME/UICC with different network environments

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 1
1	3G	3G	3G	3G	3G	yes	A
2			2G	3G	3G	yes 1) 3)	B
3							
4			2G	2G	3G	yes 2) 3)	C
5							
6			2G	3G	2G	yes 2) 3)	E
7							
8			2G	2G	2G	yes 2) 3)	D

Note: 1) requires service n° 27 supported by the USIM
2) requires services n° 27 and n° 38 supported by the USIM
3) only with 2G/3G dual mode ME

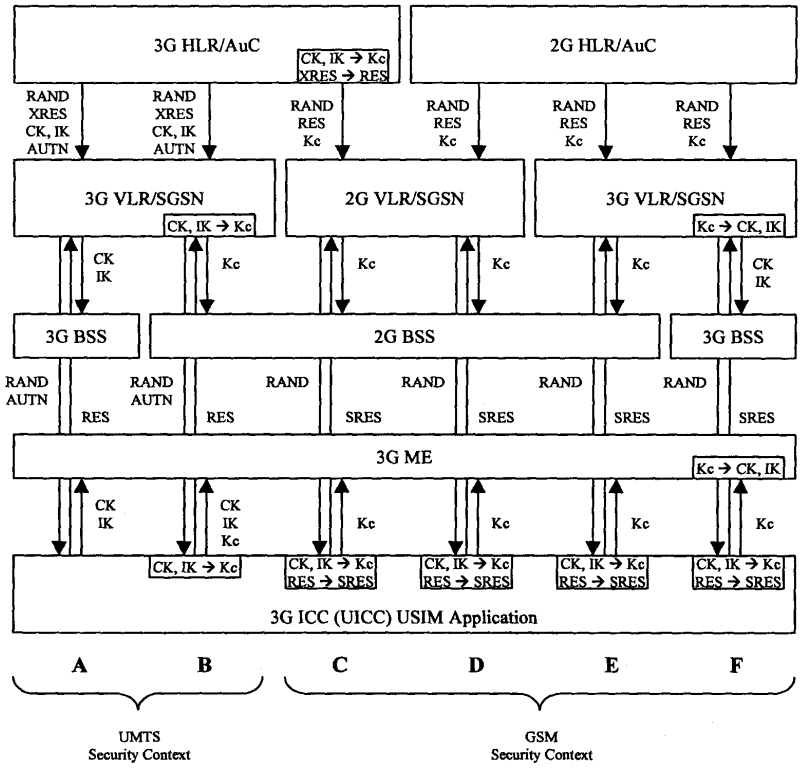


圖 14：Possible Interworking of a 3G ME and UICC with different network environment

(B) With 2G ME and UICC

當用戶使用 3G 的 UICC 卡與 2G ME 組合使用時，其必要條件是 UICC 必須支援 SIM 應用程式。

本群的組合情形，Case 1, 3, 5, 7 因爲 2G ME 無法與 3G BSS 連接，所以此 4 種組合情形並不存在。

表 15：Possible interworking scenarios of a 2G ME /UICC with different network environments

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 2
1	3G with SIM Appl.	2G					
2			2G	3G	3G	yes 1)	G
3							
4			2G	2G	3G	yes 1)	H
5							
6			2G	3G	2G	yes 1)	J
7							
8			2G	2G	2G	yes 1)	I
Note: 1) No service if UICC does not contain a SIM application							

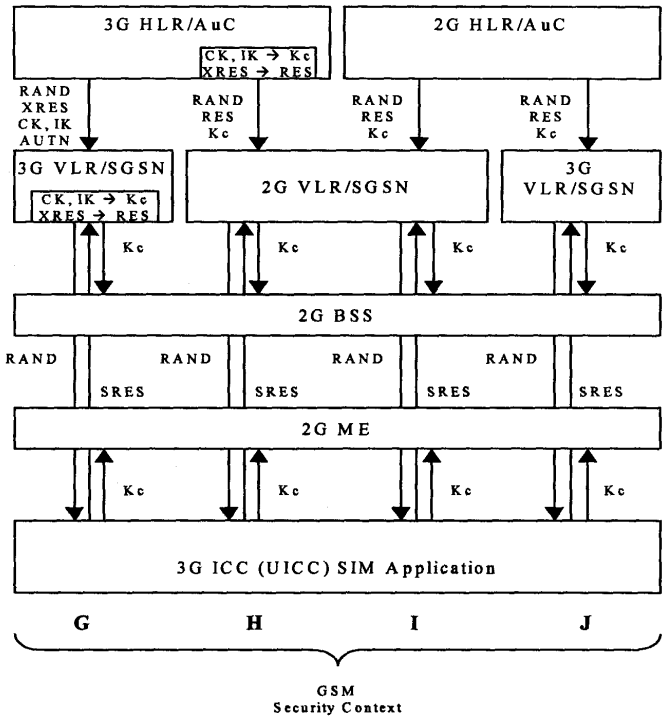


圖 15：Possible interworking scenarios of a 2G ME and UICC with different network environments

(C) With 3G ME and SIM

當用戶使用 2G 的 SIM 卡插入 3G 手機使用時，適用下列的可能組合情況，因爲 3G BSS 無法與 3G 的 VLR/SGSN 互連，所以本群 Case 3 組合情形無法搭配。

表 16：Possible interworking scenarios of a 3G ME/SIM with different network environments

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 3
1	2G	3G	3G	3G	2G or 3G	yes	K
2			2G	3G		yes 1)	L
3							
4			2G	2G		yes 1)	M
Note: 1) 2G/3G dual mode ME required							

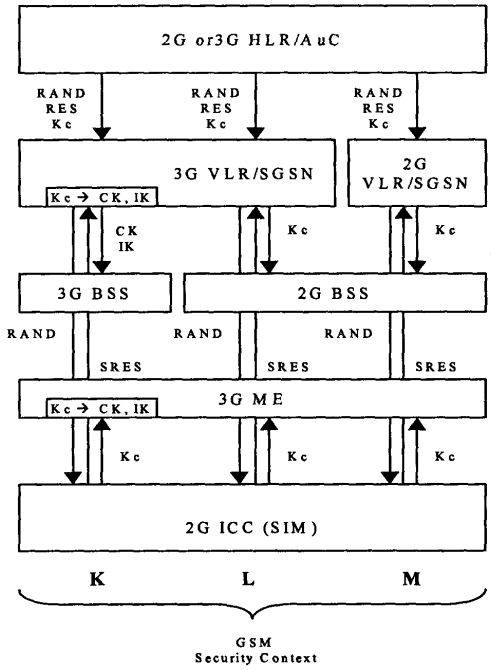


圖 16：Possible interworking scenarios of a 3G ME and SIM with different network environments

(D) With 2G ME and SIM

當用戶使用 2G ME 插入 2G SIM 卡時就是純 2G MS, 所以本群 Case 1 及 Case 3 的情形不會發生。

表 17：Possible interworking scenarios of a 2G ME/SIM with different network environments

Case	ICC	ME	BSS	VLR/SGSN	HLR/AuC	Service	Figure 4
1	2G	2G			2G or 3G		
2			2G	3G		yes	N
3							
4			2G	2G		yes	O

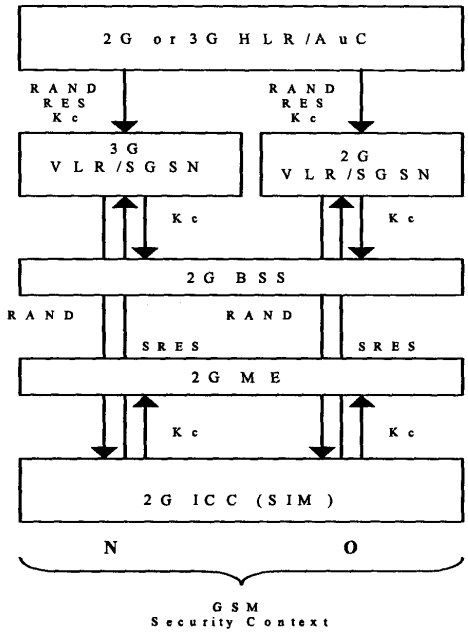


圖 17：Possible interworking scenarios of a 2G ME and SIM with different network environments

3.8 OTA 功能

OTA 功能提供經由 SMS-PP 或是 SMS-CB 兩種簡訊格式訊息進行 USIM 之遠端管理功能，TS 23.048 規範之管理功能有檔案管理與 Applet 程式管理兩種。

系統業者欲提供此功能時，除了須建置遠端管理伺服器外，UICC 卡也必須有對應之管理程式配合。

OTA 管理功能的提供對系統業者而言，提供了 USIM 遠端參數變更能力，以及彈性的加值程式服務下載機制，使易於規劃個別客戶差異化之服務。

雖然 OTA 機制提供了方便的 ICC 卡管理途徑，但是對講求系統安全的行動電話系統而言，如果沒有相當安全的管理機制，恐怕適得其反。所以本項服務功能在安全設計方面必須有相當的考量。

3.8.1 遠端檔案管理功能

遠端檔案管理功能分 Input 與 Output 兩類，前者更新 UICC 卡之檔案內容，後者可以讀取其內容。規範定義命令如下表。

(1) SIM Input Command

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEEK
INCREASE
VERIFY CHV
CHANGE CHV
DISABLE CHV
ENABLE CHV
UNBLOCK CHV
INVALIDATE
REHABILITATE

(2) SIM Output Command

Operational command
READ BINARY
READ RECORD
GET RESPONSE

(3) USIM Input Command

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEARCH RECORD
INCREASE
VERIFY PIN
CHANGE PIN
DISABLE PIN
ENABLE PIN
UNBLOCK PIN
DEACTIVATE FILE
ACTIVATE FILE

(4) USIM Output Command

Operational command
READ BINARY
READ RECORD
GET RESPONSE

3.8.2 遠端 Applet 管理功能

Applet 程式下載的程序如下圖所示，乃是經由下列多道順序之命令完成。如果 Applet 程式較大而無法由一個命令完成時，可能須由多通簡訊訊息完成。

與檔案管理功能一樣，Applet 程式管理功能也有輸入及輸出兩類。

(5) Applet Input Command

Operational command
DELETE
SET STATUS
INSTALL
LOAD
PUT KEY

(6) Applet Output Command

Operational command
GET STATUS
GET DATA

3.8.3 OTA 協定

本節說明以 SMS-PP 簡訊方式執行 OTA 功能之協定。下圖爲簡訊服務的 Protocol layer 示意圖，

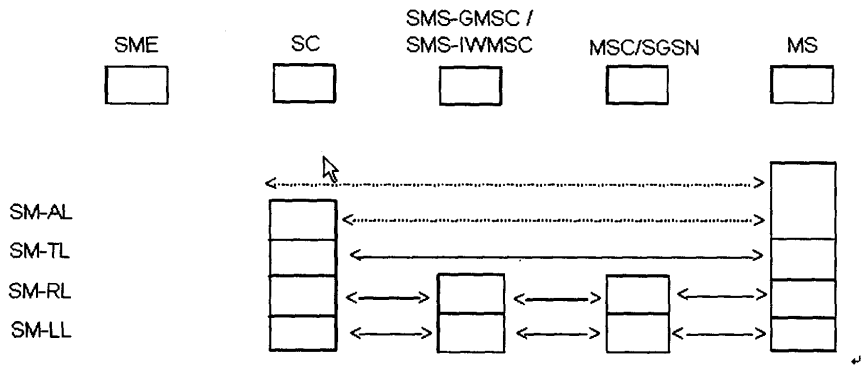


Figure 7: Protocol layer overview for the Short Message Service

下表爲 SMS-DELEVER Transport layer 之協定格式，協定格式的 TP-PID Protocol Identifier 欄位爲'7F'時定義此封簡訊爲(U)SIM Data Download 用，

當 ME 收到此種格式的簡訊訊息後，不會予以處理，而是直接以 UICC 的 ENVELOP(SMS-PP Download)命令送給 UICC 執行，並等待 UICC 的回應訊息。

表 18：Basic elements of the SMS-DELIVER

Abbr.	Reference	P (note 1)	R (note 2)	Description
TP-MTI	TP-Message-Type-Indicator	M	2b	Parameter describing the message type.
TP-MMS	TP-More-Messages-to-Send	M	b	Parameter indicating whether or not there are more messages to send
TP-RP	TP-Reply-Path	M	b	Parameter indicating that Reply Path exists.
TP-UDHI	TP-User-Data-Header-Indicator	O	b	Parameter indicating that the TP-UD field contains a Header
TP-SRI	TP-Status-Report-Indication	O	b	Parameter indicating if the SME has requested a status report.
TP-OA	TP-Originating-Address	M	2-12o	Address of the originating SME.
TP-PID	TP-Protocol-Identifier	M	o	Parameter identifying the above layer protocol, if any.
TP-DCS	TP-Data-Coding-Scheme	M	o	Parameter identifying the coding scheme within the TP-User-Data.
TP-SCTS	TP-Service-Centre-Time-Stamp	M	7o	Parameter identifying time when the SC received the message.
TP-UDL	TP-User-Data-Length	M	I	Parameter indicating the length of the TP-User-Data field to follow.
TP-UD	TP-User-Data	O	note 3	

NOTE 1: Provision; Mandatory (M) or Optional (O).

NOTE 2: Representation; Integer (I), bit (b), 2 bits (2b), Octet (o), 7 octets (7o), 2-12 octets (2-12o).

NOTE 3: Dependent on the TP-DCS.

3.8.4 OTA 安全機制

爲求安全的訊息傳送，OTA 機制必須配合安全的加密及防護機制。此項機制透過在 SMS 信息中設定 TP-UD 含有 Command Header 訊息，然後在 Command header 的下列欄位指定加密機制以及安全參數。

(A) SPI
(B) KIc
(C) KId
(D) TAR
(E) Counter

(F) PCNTR

(G) RC/CC/DC

下圖爲 SMS-PP 的 UDH

表 19：Relationship of Command Packet in UDH for single Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
UDL		Indicates the length of the entire SM.
UDHL	='02'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa (see figure 2), and is '02' in this case.
IEIa	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier. This value is reserved in TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa, which is zero, indicating that IEDa is a null field..
IEDa		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)(Note)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [8].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [8].
	Security Parameter Indicator (SPI)	see detailed coding in TS 23.048.
	Ciphering Key Identifier (KIc)	Key and algorithm Identifier for ciphering.
	Key Identifier (KID)	Key and algorithm Identifier for RC/CC/DS.
	Toolkit Application Reference (TAR)	Coding is application dependent.
	Counter (CNTR)	Replay detection and Sequence Integrity counter.
	Padding counter (PCNTR)	This indicates the number of padding octets used for ciphering at the end of the secured data.
	Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
	Secured Data	Application Message, including possible padding octets.

3.9 ADE 加值應用

USAT(Universal SIM Toolkit)是 3G 行動電話應用 USIM 提供加值應用的工

具，中華電信的 emome 理財通即是應用 GSM SAT(SIM Application Toolkit)開發之證券、轉帳、付款等之理財應用服務，這次 3G 行動電話購案的 USIM 解決方案也應使用 USAT 的標準持續提供 emome 理財通的服務。

現行 STK 應用在 SIM 卡發行後即非常沒有彈性修改使用者操作菜單或更改參數檔案，所以幾乎沒有辦法提供較動態行的服務型態，而目前行動消費服務市場又瞬息萬變，所以 STK 的應用即受到非常大的限制。OTA 即可提供一較有彈性之可修改應用服務表現方式之機制，所以本次 3G 行動電話購案亦包含 OTA 解決方案之提供。

本次中華電信 3G 行動電話購案承商 Nokia 公司提出之 OTA 解決方案爲 Gemplus 公司的 ADE 產品，以下即說明 ADE 的架構及功能。

3.9.1 ADE 簡介

ADE 的全名爲 Application Download Enabled，是 Gemplus 公司的產品，其使用 Control Blocks 的觀念來建立 USIM 上之應用程式，ADE Kernel 並依據與使用者的互動進行一系列 Control Blocks 的處理(如下圖 18)。

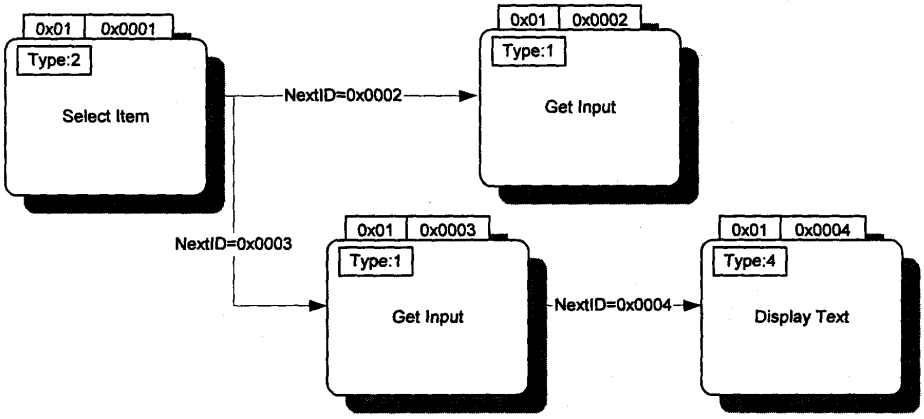


圖 18：Connections of Control blocks

3.9.2 爲何需要 ADE

現行 STK 應用在 SIM 卡發行後即非常沒有彈性修改使用者操作菜單或更改參數檔案，所以幾乎沒有辦法提供較動態行的服務型態，而目前行動消費服務市場又瞬息萬變，所以 STK 的應用即受到非常大的限制。Gemplus 公司的 ADE 產品即可克服前述限制，提供較有彈性之 USIM 應用程式開發工具。

3.9.3 ADE 功能說明

ADE 功能架構圖如下

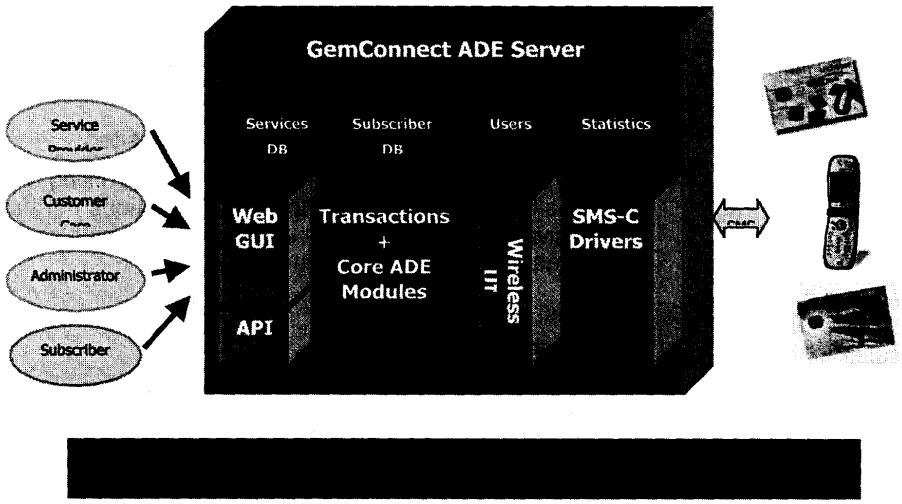


圖 19：Gemplus ADE 功能架構圖

主要功能說明如下：

(A) OTA(Over The Air)服務管理

- Allow remote ADE services download, update and removal
- Automatic OTA synchronization of subscriber environment
- Optimized OTA protocol based SMS layer

(B) 服務管理

- Comprehensive Services Repository
- Services attributes and implementation management
- Services Testing
- Service life cycle management
- Comprehensive Subscriber's database
- Management of services portfolio per subscriber
- SIM card characteristics and available resources management

(C) 訂戶自訂個人化服務組合

- GemConnect ADE allows subscribers to directly manage their owner portfolio os services

(D) 服務供應商公開介面

- GemConnect ADE Solution provides Service Provider Support
- Authorized Service Providers can develop ADE services、upload ADE services in the platform services repository and perform end-to-end testing of their services

(E) 系統與訂戶狀況統計

- Relevant data generation for statistics and reports generation can be activated at any time
- Subscribers and Services information repository
- These data allows ststem and subscribers profiling on various topics such as : number of transactions performed on a given period、top most downloaded service and latest services transaction per subscribers.

3.9.4 ADE 核心功能模組

(A) 以Web爲基礎之使用者介面

- A full set of Web-based MMI is provided : Customer care GUI for Telco's Customer Care Services、Operations and management GUI for platform administration、Service provider GUI、Subscriber's self care fully customizable GUI
- English and Chinese languages support

(B) 服務開通

- Service provisioning : through GUI and APIs
- Users provisioning including subscriber : GUI and API interfaces enables the assigning of a subscriber to a SIM card
- Subscriber : OTA/Web registration by subscriber
- Capabilities beyond creation include query, modify and delete of data

(C) 需求管理與監督

- GUI, Wireless and APIs allows request submission to the GemConnect ADE Platform
- The GUI Interface provides facilities for request submission including : Subscriber List Construct based on subscriber attributes and services、Subscriber Information Display
- GUI interface offers monitoring of ongoing requests
- Following parameters are shown per requests : submission date、sneder of the request、subscriber's MSISDN、type of the service and status of the request
- Requests can be filtered with respect to each of the above

(D) 支援多家簡訊中心介面

- SMSC from Logica, CMG, Nokia, Sema

- SMPP interface de facto standard is full supported
- CMPP and SGIP interfaces
- Others can be supported o demand

(E) 紀錄

- Powerful and configurable logging tool
- System information messages(including errors) are output to dedicated log files in a structured formats.

4. 建議

從 SIM 進入 USIM 時代，即表示 GSM 行動電話從 2G 進入到 3G 的網路與服務，第三代行動電話時代所提供之行動通信服務將更多元化。

本分公司 emome 理財通服務已在行動加值服務跨出重要的一步，3G 系統平台的寬頻特性以及未來 Bearer independent protocol 規範更斟成熟時，搭配 3G 完善的系統安全機制以及 UICC 卡的 Multi application 架構平台，相信與生活結合在一起的各種行動加值應用將更爲發達，也更爲大眾所接受。

因應前述預期趨勢，有關第三代行動電話網路與 WLAN(Wireless Local Area Network)網路的整合議題、USIM 與 WPKI(Wireless Public Key Infrastructure)及 JSR-177(Security and Trust Services API for J2ME Technology)等安全應用基礎之加值服務研發將是未來相關單位研討之重要課題。

5. 參考資料

1. 3GPP TS 21.111 USIM and IC card requirements
2. 3GPP TS 22.038 USIM/SIM application t toolkit(USAT/SAT) ;Service description1
3. 3GPP TS 23.002 Network architecture
4. 3GPP TS 23.040 Technical realization of Short Message Service
5. 3GPP TS 23.048 Security Mechanisms for the U(SIM) application toolkit
6. 3GPP TS 31.101 UICC-Terminal Interface; Physical and Logical Characteristics
7. 3GPP TS 31.102 Characteristics of the USIM Application
8. 3GPP TS 31.111 USIM application toolit(USAT)
9. 3GPP TR 31.900 SIM/USIM internal and external interworking aspects
10. 3GPP TR 33.909 Report on the design and evaluation of the Milenage Algorithm Set
11. 3GPP TS 33.102 Security architecture
12. 3GPP TS 33.105 Cryptographic algorithm requirements
13. 3GPP TS 35.205 Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*;Document 1: General
14. 3GPP TS 35.206 Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*;Document 2: Algorithm Specification
15. Training Documents of Gemplus

6. Abbreviations

In addition to (and partly in overlap to) the abbreviations included in TR 21.905, for the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI

Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number
SQNHE	Individual sequence number for each user maintained in the HLR/AuC
SQNMS	The highest sequence number the USIM has accepted
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response