200915814

双面影印

# 發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

**※ 申請案號：** 97125032

**※ 申請日期：** 97.7.3 **※IPC 分類：** H04L 9/08 (2006.01)
H04L 9/12 (2006.01)

## 一、發明名稱：（中文/英文）

用於金鑰參數供應的方法、裝置、系統、與電腦程式

METHOD, APPARATUS, SYSTEM AND COMPUTER PROGRAM FOR KEY PARAMETER PROVISIONING

## 二、申請人：（共 1 人）

**姓名或名稱：**（中文/英文）

諾基亞股份有限公司 / NOKIA CORPORATION

**代表人：**（中文/英文）

鴻卡薩洛　哈利 / HONKASALO, HARRI

**住居所或營業所地址：**（中文/英文）

芬蘭艾斯浦・克萊萊登堤 4 號

Keilalahdentie 4, 02150 ESPOO, Finland

**國　籍：**（中文/英文）

芬蘭 / FINLAND

## 三、發明人：（共 2 人）

**姓　名：**（中文/英文）

1. 布隆馬特　馬克 / BLOMMAERT, MARC
2. 荷特曼斯　西爾克 / HOLTMANNS, SILKE

**國　籍：**（中文/英文）

1. 比利時 / BELGIUM
2. 丹麥 / DENMARK

## 四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國、　2007/07/03、　60/929,589

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

## 九、發明說明：

### 【發明所屬之技術領域】

發明領域

本發明之示範性實施例一般是關於鑑別及安全性技術，本發明尤其是關於使用利用一通用自舉架構(GBA)服務的任何網路應用功能(NAF)及使用者設備(UE)之金鑰參數供應。特別地，多媒體廣播/多播服務(MBMS)、行動TV(電視)及裝置管理是依據本發明之示範性實施例的金鑰參數供應可在其內被部署的示範性服務。

### 【先前技術】

發明背景

現在行動經營者要求提供行動TV服務的第三世代合作計畫(3GPP)MBMS系統。出於安全目的，一MBMS可使用3GPP通用自舉架構(GBA)或廣播方案，其等一般包含網際網路協定(IP)TV及應用(例如，機上盒)，其等也可使用GBA之衍生物，例如擴充細節以支持核心或其他特定網路。

3GPP通用鑑別架構(GAA)是基於3GPP之行動演算法AKA(鑑別及金鑰同意協定)以及3GPP2之詢問-握手鑑別協定(CHAP)以及蜂巢鑑別及語音加密(CAVE)。GBA也適用於(例如)纜線網路經營者之特定需求且考慮他們的安全協定喜好。開放式行動聯盟(OMA)廣播內容保護及多媒體廣播多播服務之GBA的使用導致產生一新的3GPP GBA規格(技術規格(TS)33.223 GBA推入)。GBA是基於一網路與一裝置的安全特徵。

在3GPP TS 33.220中(例如，自舉伺服器功能(BSF)、GBA)章節4.4.11中，以下定義被給出:

“當提到GBA金鑰時，以下金鑰被指定：Ks自該Ks導出的NAF特定金鑰。

當提到NAF特定金鑰時，以下金鑰被指定：Ks_ext/int_NAF(在GBA_U(具有基於通用積體電路卡(UICC)增強的GBA)脈絡中)(...)，以及自該等金鑰導出的任何金鑰。

符號Ks_(ext/int)_NAF表示GBA_U(...)脈絡中的Ks_ext/int_NAF。

符號Ks_(ext)_NAF表示GBA_U(...)脈絡中的Ks_ext_NAF。

依據3GPP TS 33.223章節3.1及4.3.9，詞語GBA-PUSH-INFO可包含用於GBA推入中的金鑰導出之相關資料，如AUTN(*)、RAND、NAF_ID、B-TID。GBA-PUSH-INFO可經由如Upa-參考點從NAF發送到UE。此外，自舉異動識別符(B-TID)可被包含(例如)在該推入訊息內以校正GBA-PUSH-INFO與被自GBA-PUSH-INFO產生的安全結合保護的推入訊息之可能的反向順序情形(在該GBA-PUSH-INFO及推入訊息被個別發送之情形下)。即，B-TID可使用，例如作為被用於參考點Upa及Ua(將在以下被描述)的協定中的金鑰識別符。

在3GPP TS 33.233內，目前假設識別密碼金鑰的自舉異動識別符(B-TID)被用於Ua-訊息識別(例如，參看SA3#47

S3-070456之3GPP會議文件)且另外以Upa-訊息被傳輸。3GPP TS 33.233不包括Upa內的任何使用者識別。此外，可假設一UE身分與該Upa訊息一起被傳輸，該Upa訊息是用以遞送至少該GBA-PUSH-INFO的訊息。

## 【發明內容】

發明概要

在一第一層面中，本發明之示範性實施例提供一種方法，該方法包括以下步驟：接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；加密至少核心網路相關動態身分資訊；以及以該金鑰產生相關資訊回復該查詢，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

在另一層面中，本發明之示範性實施例提供一種被組配以儲存程式指令的記憶體媒體。該等程式指令之執行導致執行包含以下步驟的操作：接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；加密至少核心網路相關動態身分資訊；以及以該金鑰產生相關資訊回復該查詢，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

在另一層面中，本發明之示範性實施例提供一種裝置，包括：一接收器，被組配以接收使用者設備處理指令資訊以及金鑰產生相關資訊之一請求；一產生器，被組配

以產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；一加密器，被組配以加密至少核心網路相關動態身分資訊；以及一發送器，被組配以以該金鑰產生相關資訊回應該請求，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

在又一層面中，本發明之示範性實施例提供一種裝置，包括：用於接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢的裝置；用於產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊的裝置；用於加密至少核心網路相關動態身分資訊的裝置；以及用於以該金鑰產生相關資訊回復該查詢的裝置，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

在另一層面中，本發明之示範性實施例提供一種方法，包括以下步驟：接收使用者設備處理指令資訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；解密該被接收的已加密核心網路相關動態身分資訊；以及基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

在另一層面中，本發明之示範性實施例提供一種被組配以儲存程式指令的記憶體媒體。該等程式指令之執行導致執行包含以下步驟的操作：接收使用者設備處理指令資

訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；解密該被接收的已加密核心網路相關動態身分資訊；以及基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

在又一層面中，本發明之示範性實施例提供一種裝置，包括：一接收器，被組配以接收使用者設備處理指令資訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊；一產生器，被組配以產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；以及一解密器，被組配以解密該被接收的已加密核心網路相關動態身分資訊以用於基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

在又一層面中，本發明之示範性實施例提供一種裝置，該裝置包含：用於接收使用者設備處理指令資訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊的裝置；用於產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊的裝置；用於解密該被接收的已加密核心網路相關動態身分資訊的裝置；以及用於基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊的裝置。

在又一層面中，本發明之示範性實施例提供一種方法，包括以下步驟：接收使用者設備處理指令資訊以及一通用自舉架構推入資訊(GPI)之一查詢；產生與該被接收的

使用者設備處理指令資訊有關的第一金鑰資訊(Ks_(ext/int)_BSF)；加密至少一網路應用功能域名伺服器(NAF DNS)名稱，其中該GPI之一E_GPI部分包含該已加密NAF DNS名稱；以及以該E_GPI及被接收的使用者設備處理指令資訊答復該查詢。

在又一層面中，本發明之示範性實施例提供一種方法，包括以下步驟：接收一訊息，該訊息包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)以及使用者設備處理指令資訊，其中該GPI之一E_GPI部分包含一已加密網路應用功能域名伺服器(NAF DNS)名稱；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊(Ks_(ext/int)_BSF)；解密該被接收的已加密NAF DNS名稱；以及基於該已解密NAF DNS名稱導出第二金鑰資訊(Ks_(ext/int)_NAF)。

圖式簡單說明

本發明之示範性實施例在以下參看附圖被描述，其中：

第1圖顯示了用於依據本發明之示範性實施例的金鑰參數供應之個別方法；以及

第2圖顯示了用於依據本發明之示範性實施例的金鑰參數供應之個別裝置(例如，一使用者設備及NAF/BSF)。

## 【實施方式】

較佳實施例之詳細說明

需注意到的是，對於本說明書，縮寫詞GPI (GBA推入資訊)、Ks_(ext/int)_BSF、Ks_(ext)NAF 、NAF DNS名稱等

是儲存在一資料庫內的金鑰產生相關資訊、第一金鑰資訊、第二金鑰資訊、核心網路相關動態身分資訊以及獨特使用者身分資訊以供進一步的安全目的(如分別用於鑑別或應用安全等)，未將後面的詞語限於施加給該等縮寫詞或者被用於服務特定金鑰導出(即Ks_(ext/int)_NAF)之基線憑證之特定技術或實施態樣細節。

本發明之示範性實施例現在參考第1及2圖被描述。

首先，然而，需注意到的是，GBA推入之一主要特徵以及與3GPP TS 33.220概述的GBA之差異可被考量以涵蓋3GPP TS 33.223可自舉用於廣播網路之金鑰的事實，即單方向使用，例如至少一網路節點與一UE或終端機之間的一安全結合之網路初始化建立，作為一例子。然而，一廣播網路內的GBA推入之使用需要與被用於3GPP TS 33.220中的金鑰導出技術有關的特別考量。此等層面中的一者可以是被用於密碼金鑰導出的NAF名稱。無法假設所有廣播網路都對所謂的頭端使用基於領域名稱伺服器(DNS)名稱，在它們作為一發送GBA推入訊息的NAF之情況下。單向模式的GBA推入之使用沒有排除可能具有該UE可使用的一可能的後頻道之情形，例如若金鑰遞送不成功。

例如，當在一網際網路協定(IP)網路(例如數位視訊廣播-手持(DVB-H))上執行廣播時，沒有使用DNS名稱。此外，可假設一使用者無法執行一上行鏈路反向DNS查詢以解出與源IP位址相關的DNS名稱。而且，DVB-H中使用的EPG(電子節目指南)不包含一IP位址對DNS名稱之映射資訊。

因此，明確的DNS名稱傳輸(與Ua安全協定識別符一起，當其無法藉由其他方式被導出時)可被認為是此問題之一解決方法，且可維持GBA推入解決方法與UE初始化GBA概念之一些相容性。

然而，若當使用者身分與NAF ID在廣播網路上傳播時都清楚可見時，則傳輸該NAF識別符(簡而言之，NAF-ID、NAF DNS名稱以及Ua協定ID)可能造成一隱私問題。此操作之類型可使追蹤使用者行為成為可能，因此可能讓人討厭。

鑑於上述，本發明之示範性實施例提供增強金鑰參數供應。

例如，一第一方法可包括：

對一特定使用者設備，接收金鑰產生相關資訊之一查詢及使用者設備處理指令資訊；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

基於該產生的金鑰資訊加密至少核心網路相關動態身分資訊；以及

發送包含至少該已加密核心網路相關動態身分資訊及該被接收的使用者設備處理指令資訊的金鑰產生相關資訊。

該方法可進一步包括以下步驟：獲得一鑑別向量，該鑑別向量包含一隨機數及密碼金鑰內容中的一者；以及導出接著用於該金鑰資訊之產生的通用金鑰資訊。該方法可進一步包括以下步驟：自一使用者資料庫獲得一使用者身分符記；以及導出接著用於該第一金鑰資訊之產生的通用

金鑰資訊。該被接收的使用者設備處理指令資訊可進一步包含一行動應用識別符，以及該方法可進一步包含基於該被接收的使用者設備處理指令資訊產生第二金鑰資訊。

進一步依據本發明之示範性實施例，一第二方法包含以下步驟：

接收包含至少已加密核心網路相關動態身分資訊及使用者設備處理指令資訊的金鑰產生相關資訊；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

基於該產生的第一金鑰資訊解密該被接收的已加密核心網路相關動態身分資訊；以及

基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

該方法可進一步包括以下步驟：當接收時接收一第一金鑰產生識別符，以及當產生時產生也與被接收的金鑰產生識別符有關的該第一金鑰資訊。一第一金鑰產生識別符可被預先組配，且當產生時，與該被預先組配的金鑰產生識別符有關的第一金鑰資訊也可被產生。當接收時，一Ua訊息被接收，且該方法進一步包含基於該導出的第二金鑰資訊處理被接受的訊息，且該Ua訊息利用該金鑰產生相關資訊被保護且封裝。

進一步依據以上方法，核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器名稱以及一Ua介面協定識別符中的至少一者。該金鑰產生相關資訊可包含以下中

的至少一者：一獨特使用者識別符；一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

進一步依據該等示範性實施例，可具有基於該鑑別符記產生通用金鑰資訊之一步驟，以及該方法可進一步包括基於該第一金鑰資訊鑑別該通用自舉架構推入資訊之完整性保護部分。

以上方法可被執行為被儲存在任何適合類型的電腦可讀記憶體媒體內的電腦程式指令之執行的一結果。

該等示範性實施例進一步包括一第一裝置，該第一裝置包括一接收器，該接收器被組配以對一特定使用者設備接收金鑰產生相關資訊之一查詢及使用者設備處理指令資訊；一產生器，被組配以產生與被該接收器接收的該使用者設備處理指令資訊有關的第一金鑰資訊；一加密器，被組配以基於該產生器產生的該金鑰資訊加密至少核心網路相關動態身分資訊；以及一發送器，被組配以發送該金鑰產生相關資訊，該金鑰產生相關資訊包含被該加密器加密的至少該核心網路相關動態身分資訊以及被該接收器接收的該使用者設備處理指令資訊。

該裝置可進一步包括一獲得器及一導出器，該獲得器被組配以獲得一包含一隨機數以及密碼金鑰內容的鑑別向

量，該導出器被組配以導出接著用於被組配以產生該金鑰資訊的產生器之通用金鑰資訊。

該裝置可進一步包含一獲得器，該獲得器被組配以自一使用者資料庫獲得一使用者身分符記；以及一導出器，被組配以導出接著用於被組配以產生該第一金鑰資訊的產生器之通用金鑰資訊。

被該接收器接收的使用者設備處理指令資訊可進一步包含一行動應用識別符，以及其中該產生器被進一步組配以產生與被該接收器接收的該使用者設備處理指令資訊有關的第二金鑰資訊。

該等示範性實施例進一步包括一第二裝置，該第二裝置包括一接收器，該接收器被組配以接收包含至少已加密核心網路相關動態身分資訊及使用者設備處理指令資訊的金鑰產生相關資訊；以及一產生器，被組配以產生與被該接收器接收的該使用者設備處理指令資訊有關的第一金鑰資訊；一解密器，被組配以基於該產生器產生的該第一金鑰資訊解密被該接收器接收的該已加密核心網路相關動態身分資訊；以及一導出器，被組配以基於被該解密器解密的該核心網路相關動態身分資訊導出該第二金鑰資訊。

進一步依據此層面，該接收器被進一步組配以接收一第一金鑰產生識別符，以及該產生器被進一步組配以產生也與該接收器接收的該金鑰產生識別符有關的第一金鑰資訊。一第一金鑰產生識別符被預先組配，以及該產生器被進一步組配以產生也與該被預先組配的金鑰產生識別符有

關的第一金鑰資訊。

該接收器被進一步組配以接收一Ua訊息，以及該裝置另外包含一處理器，該處理器被組配以基於導出的第二金鑰資訊處理被該接收器接收的訊息。

該裝置可包含一通用積體電路卡及一安全記憶體中的一者，以及一介面，該介面被組配以提供該金鑰產生相關資訊中的至少一部分給該通用積體電路卡或該安全記憶體。

與以上裝置相關，該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器名稱以及一Ua介面協定識別符中的至少一者；以及該金鑰產生相關資訊包含以下中的至少一者：一獨特使用者識別符；至少一隨機數及一正負號結果中的一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；被導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定(GUSS)。該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

該第二裝置可進一步包含一創建器，該創建器被組配以基於該鑑別符記產生通用金鑰資訊；以及一鑑別器，該鑑別器被組配以基於該第一金鑰資訊鑑別該通用自舉架構推入資訊之該完整性保護部分。

該第一裝置可由一自舉伺服器功能及一網路應用功能中的一者組成，同時該第二裝置可由一使用者設備、一行動設備及一通用積體電路卡中的一者組成。

進一步依據該等示範性實施例，另一裝置包括用於對

一特定使用者設備接收金鑰產生相關資訊之一查詢及使用者設備處理指令資訊的裝置；用於產生與被該用於接收的裝置接收的該使用者設備處理指令資訊有關的第一金鑰資訊的裝置；用於基於該用於產生的裝置產生的該金鑰資訊加密至少核心網路相關動態身分資訊的裝置；以及用於以發送該金鑰產生相關資訊的裝置，該金鑰產生相關資訊包含被該用於加密的裝置加密的至少該核心網路相關動態身分資訊以及被該用於接收的裝置接收的該使用者設備處理指令資訊。

進一步依據該等示範性實施例，又一裝置包括用於接收包含至少已加密核心網路相關動態身分資訊以及使用者設備處理指令資訊的裝置；用於產生與被該用於接收的裝置接收的該使用者設備處理指令資訊有關的第一金鑰資訊的裝置；用於基於該用於產生的裝置產生的該金鑰資訊解密被該用於接收的裝置接收的該已加密核心網路相關動態身分資訊的裝置；以及用於基於該用於解密的裝置解密的該核心網路相關動態身分資訊導出第二金鑰資訊的裝置。

該等示範性實施例之使用提供一些優點。例如，不需要將源IP位址從該IP層傳遞到一GBA客戶端，因此不需要具有層間通訊。

進一步舉例，該等示範性實施例之使用提供對NAF之IP位址的變化之不敏感性，因此可應用於(例如)其IP位址可能經常變化之具有不好的連接性的網路。

進一步舉例，該等示範性實施例之使用提供NAF之位

置的不變性。例如，若(例如)該NAF在一防火牆後或一網路位址解譯遍歷伺服器被使用，則鄰近伺服器及防火牆沒有引起一額外的問題。

進一步舉例，該等示範性實施例之使用提供DoS(服務拒絕)攻擊之減輕(因為核心IP位址容易受到此等DoS攻擊之危害)。

進一步舉例，該等示範性實施例之使用去除了兩個Ua端點都實施一額外金鑰導出機制以及基於使用情形在它們之間選擇的需要。

進一步舉例，該等示範性實施例去除了(例如)對一終端機內的一智慧卡(例如，UICC)進行改變之需要。

第1圖顯示了依據本發明之示範性實施例的金鑰參數供應之個別方法。元件之間的發訊在水平方向被指出，而發訊之間的時間層面以發訊順序之垂直配置以及序號被反映。

如第1圖所示，一通訊系統100可包含一接取網路104及使用者設備UE 102。該接取網路104接著可包含一網路應用功能NAF 101、一自舉伺服器功能BSF 103以及一用於提供一接取技術給該UE 102的可取捨基地台BS 104，如本文以下所描述的。需注意到的是，該NAF 101及該BSF 103可以是經由Zpn介面點通訊的獨立功能，例如在該接取網路104內。可選擇的方式是，該NAF 101及該BSF 103也可以是包含在(例如)一個單一伺服器內的功能(由該NAF 101及該BSF 103之符號周圍的一虛線方塊指出)。作為又一選擇，該BSF 103可被組配以作為一NAF 101。若該BSF 103及該

NAF 101被設置在一起，則該Zpn參考點可被刪除。並不限於此，為了簡化描述，以下描述只闡述了後一選擇，且參考符號"NAF/BSF 101"被用於描述作為NAF 101的BSF 103。

除此之外，該NAF 101及該UE 102可被組配以經由Ua參考點傳遞(例如)一應用協定，以及經由Upa參考點傳遞一AKA協定。該BS 104可設於該NAF 101與該UE 102之間的信號路徑內以提供與感興趣的接取技術之符合性。

如第1圖中所示，依據一第一方法，在步驟S1-1中，該NAF 101(或NAF/BSF 101)可對一特定使用者設備執行金鑰產生相關資訊(例如，一GBA-PUSH-INFO GPI)之一查詢以及使用者設備處理(安全)指令資訊(例如，Upa使用之一指示)。

在步驟S1-2中，該NAF 101可執行產生與該被接收的使用者設備處理指令資訊(例如，Upa用途之指示)有關的第一金鑰資訊(例如，Ks_(ext/int)_BSF)之步驟。作為此第一金鑰導出程序之一可取捨的輸入，具有幾個不同的可能性。例如，該BSF 103名稱(以及指定的特定Ua協定身分)，或任何其他一般已知(非私密資訊破解)資訊(或預先組配的資訊)可被使用，只要其符合NAF-ID格式(因此不需要改變(例如)在3GPP Release 6或3GPP Release 7下發證的智慧卡，或者若以如2G GBA TR 33.920類似的方式被使用，則不需改變用戶身分模組SIM卡)。該金鑰導出可在該BSF 103中被執行。

在步驟S1-3中，該NAF 101可執行加密至少核心網路相

關動態身分資訊(例如，加密該NAF DNS名稱，導致GPI之一加密部分，之後被稱為“E_GPI”)。該E_GPI也可包含(例如)未加密資訊。例如，關於選擇自舉ME或UICC(Upa-使用)之端點的資訊，或者(例如)關於基於產生的金鑰資訊(例如，Ks_(ext/int)_BSF)的端點(例如，永久性或短期金鑰)之自舉類型的資訊。

在步驟S1-4，該NAF 101可執行將包含至少該已加密核心網路相關動態身分資訊(例如，已加密NAF DNS名稱)及該被接收的使用者設備處理指令資訊)的金鑰產生相關資訊(例如，推入GPI)發送給該UE 102。

依據一第二方法，該UE 102在步驟S2-1中可執行接收至少包含該已加密核心網路相關動態身分資訊(例如，包含該已加密NAF DNS名稱的E_GPI)及該使用者設備處理指令資訊(例如，Upa使用之指示)的金鑰產生相關資訊(例如，由該NAF/BSF 101推入的GPI)。

在步驟S2-2中，該UE 102可執行產生與該被接收的使用者設備處理指令資訊有關的(例如，與Upa使用之指示有關的)第一金鑰資訊(例如，存在該UE 102內的一UICC上的Ks_(ext)_BSF)。作為此第一金鑰導出之可取捨的輸入，可能具有不同的可能性。例如，該BSF名稱(以及指定的特定Ua協定身分)或任何其他一般已知(非私密資訊破解)資訊，或預先組配的資訊可被使用，只要其符合NAF-ID格式(因此不需要改變(例如)在3GPP Release 6或3GPP Release 7下發證的智慧卡，或者以如2G GBA TR 33.920類似的方式被使

用)。應該注意到的是，該BSF名稱作為一非限制性例子被使用。

在步驟S2-3中，該UE 102可基於該產生的第一金鑰資訊(如Ks_(ext)_BSF)執行解密該被接收的已加密核心網路相關動態身分資訊(例如，解密E_GPI，導致該NAF/BSF 101之DNS名稱)。

在步驟S2-4中，該UE 102可基於該已解密核心網路相關動態身分資訊(例如該NAF/BSF 101之DNS名稱)執行導出第二金鑰資訊。

依據以上第一方法之進一步的實施例以及細化，在步驟S1-1-1中，該NAF/BSF 101可進一步執行獲得一鑑別向量(AV)，該AV包含(例如)被用於進一步應用特定憑證之主金鑰資料(之後也被稱為密碼金鑰內容)，包含至少一隨機數(RAND)、一鑑別符記(AUTN)、一被期望的回應(XRES)、一密鑰(CK)以及一完整性金鑰(IK)，且導出通用金鑰資訊(例如，Ks)以供接著用於產生金鑰資訊(例如，Ks_(ext/int)_BSF)可被執行。可選擇的方式是，一使用者身分符記可在以上描述的獲得期間被獲得。除此之外，該被接收的使用者設備處理指令資訊可進一步包含一行動應用識別符(例如，Ua-appli-id)，使得在步驟S1-2-1中，該NAF/BSF 101可基於該被接收的使用者設備處理指令資訊執行產生第二金鑰資訊(例如，Ks_(ext/int)_NAF)。

除此之外，在該第一及第二方法中，該核心網路相關動態身分資訊可包含一網路應用功能領域名稱伺服器

(NAF DNS)名稱及/或一Ua介面協定識別符。此外，該金鑰產生相關資訊(例如，GPI)可包含一獨特使用者識別符，例如網際網路協定多媒體子系統私人使用者身分(IMPI)、網際網路協定多媒體子系統公共使用者身分(IMPU)或其他使用者識別符、至少一隨機數(RAND)或一正負號結果(SRES)、密碼金鑰內容、通用自舉架構推入資訊之以上提到的已加密部分(E_GPI)、該通用自舉架構推入資訊之一完整性保護部分(之後稱為I_GPI)、導出的第一及第二金鑰(Ks_(ext/int)_NAF)、一金鑰壽命及/或至少一通用自舉架構使用者設定(GUSS)。而且，該使用者設備處理指令資訊可包含指示Upa使用的至少一未加密資訊元件(例如，一位元)。

除此之外，依據以上第二方法之進一步的實施例以及細化，在步驟S2-1-1中，該UE 102可進一步基於該隨機數及該鑑別符記執行產生通用金鑰資訊(Ks)。此外，在步驟S2-2-1中，該UE 102可基於該第一金鑰資訊執行鑑別該通用自舉架構推入資訊之完整性保護部分(I_GPI)。可選擇的方式是，當接收時(步驟S1-1)，一第一金鑰產生識別符可被接收，且在產生步驟中，與該被接收的金鑰產生識別符有關的第一金鑰資訊也可被產生。可選擇的方式是，該第一金鑰產生識別符可被預先組配，以及在產生(步驟S1-2)中，與該被預先組配的金鑰產生識別符有關的第一金鑰資訊也可產生。作為另一選擇，例如該UE 102可進一步執行一Ua訊息之接收，以及在步驟S2-5中，該UE 102可進一步基於

導出的第二金鑰資訊(Ks_(ext)_NAF)執行處理該被接收的訊息(例如，Ua訊息)。

第2圖顯示了依據本發明之示範性實施例的用於金鑰參數供應之個別裝置(例如，NAF/BSF 101及使用者設備UE 102)。作為一例子，該UE 102可以是一可接取該接取網路104之IP能力的終端機，其中該UE 102可進一步包含一給定形式的安全模組，例如一智慧卡、一獨立晶片或一安全軟體模組。

如第2圖中所示，該NAF 101(或者作為該NAF 101的BSF 103)可包含一中央處理單元CPU 1011、一記憶體1012、一發送器(Tx)1013、一接收器(Rx)1014、一產生器1015、一加密器1016、一可取捨的導出器1017以及至少一可取捨的額外CPU 1011a。需注意到的是，之後為了描述簡潔起見，對該NAF/BSF之CPU 1011的每個參考也可指該至少一可取捨的額外CPU 1011a中的至少一者。

如該CPU 1011之功能方塊的虛線範圍所指示，該產生器1015、該加密器1016及該可取捨的導出器1017可被實施(例如)為在該CPU 1011上執行的軟體或個別實體。需注意到的是，該發送器1013及該接收器1014之功能可以是如第2圖中所示的個別實體，或者可選擇地由一積體收發器(圖未示)執行。

該CPU 1011可被組配以處理各種資料輸入以及控制該記憶體1012、該發送器1013、該接收器1014、該產生器1015、該加密器1016、該可取捨的導出器1017以及該至少

一額外可取捨CPU 1011a之功能。該記憶體1012可用以儲存當在該CPU 1011上執行時，用於執行依據本發明之示範性實施例的個別方法之程式指令碼(較一般的是程式碼裝置)。

如結合依據本發明之實施例的個別方法所描述的，該NAF/BSF 101之接收器1013可被組配以接收金鑰產生相關資訊(例如，GPI)之一查詢以及使用者設備處理指令資訊(例如，Upa使用之指示)。

需注意的是，該查詢可源於該接取網路104內的另一網路元件(圖未示)。

該NAF/BSF 101之產生器1015可被組配以產生與該接收器1013接收的使用者設備處理指令資訊有關的第一金鑰資訊A1(例如，Ks_(ext/int)_BSF)。

該NAF/BSF 101之加密器1016接著可被組配以基於該產生器1015產生的該金鑰資訊A1加密至少核心網路相關動態身分資訊(動態ID資訊，例如加密該NAF/BSF 101之DNS名稱，導致E_GPI)。

該NAF/BSF 101之發送器1014可被組配以發送包含被該加密器1015加密的至少該核心網路相關動態身分資訊(已加密動態ID資訊)以及被該接收器1013接收的該使用者設備處理指令資訊(例如，Upa使用之指示符)的金鑰產生相關資訊(例如，GPI)。

也如第2圖中所示，該UE 102可包含一CPU 1021、一記憶體1022、一發送器(Tx)1023、一接收器(Rx)1024、一產生器1025、一解密器1026、一導出器1027、一可取捨創建

器1028、一可取捨鑑別器1029以及一可取捨介面(I/F)10210。

如該CPU 1021之功能方塊之虛線範圍所指示，該產生器1025、該解密器1026、該導出器1027、該可取捨創建器1028、該可取捨鑑別器1029以及該可取捨介面10210可被實施為在該CPU 1021上執行的軟體或者作為個別實體。需注意到的是，該發送器1023及該接收器1024之功能可以是如第2圖中所示的獨立實體，或者可選擇地由一積體收發器(圖未示)執行。

該CPU 1021可被組配以處理各種資料輸入以及控制該記憶體1022、該發送器1023、該接收器1024、該產生器1025、該解密器1026、該導出器1027、該可取捨創建器1028、該可取捨鑑別器1029以及該可取捨介面10210之功能。該記憶體1022可用以儲存當在該CPU 1021上執行時，用於執行(例如)依據本發明的個別方法之程式裝置。

如結合依據本發明之示範性實施例的個別方法所描述的，該UE 102之接收器1023可被組配以用於一特定使用者設備接收包含至少已加密核心網路相關動態身分資訊(例如，E_GPI，已加密NAF/BSF DNS名稱)及使用者設備處理指令資訊(例如，Upa使用之指示)的金鑰產生相關資訊(例如，GPI)。作為一選擇，該UE 102之接收器1023可進一步被組配以接收一Ua訊息。

需注意到的是，此可取捨訊息(msg)可源於該NAF/BSF 101。在此情況下，產生、解密、導出以及處理之後續操作

可能產生該訊息(msg)之一成功的整體處理。可選擇的方式是，該訊息(msg)可源於該通訊系統100內的另一NAF/BSF 101。在此情況下，產生、解密、導出以及處理之後續操作可能部分或完全失敗，因此導致該可取捨訊息(msg)之一不成功的整體處理。

該UE 102之產生器1025可被組配以產生與該接收器1023接收的使用者設備處理指令資訊(例如，Upa使用之指示)有關的第一金鑰資訊A2(例如，Ks_(ext)_BSF)。

該UE 102之解密器1026可被組配以接著基於該產生器1025產生的該第一金鑰資訊A2解密被該接收器1023接收的該已加密核心網路相關動態身分資訊(例如，解密E_GPI，導致NAF DNS名稱)。

該UE 102之導出器1027可被組配以基於被該解密器1026解密的核心網路相關動態身分資訊(例如，NAF DNS名稱)導出第二金鑰資訊B2(例如，Ks_(ext)_NAF)。

依據以上NAF/BSF 101之進一步的實施例，例如，該CPU 1011結合該NAF/BSF 101之記憶體1012(組成可被認為是一獲得器的東西)一起可進一步被組配以獲得一鑑別向量(AV)，該AV包含被用於進一步的特定應用憑證的主金鑰資料(也被稱為密碼金鑰內容)，包含至少一隨機數(RAND)、一鑑別符記(AUTN)、一被期望的回應(XRES)、一密鑰(CK)及一完整性金鑰(IK)中的至少一者。該可取捨導出器1017可被組配以導出通用金鑰資訊(例如，Ks，由虛線鑰匙符號指示)以接著用於被組配以產生金鑰資訊A1(例

如，Ks_(ext/int)_BSF)的產生器1015。可選擇的方式是，該獲得器可被組配以獲得一使用者身分符記。除此之外，該被接收的使用者設備處理指令資訊可進一步包含一行動應用識別符(例如，Ua-appli-id)，使得該產生器1015可進一步被組配以基於該被接收的使用者設備處理指令資訊產生第二金鑰資訊B1(例如，Ks_(ext/int)_NAF)。作為一選擇，該通用金鑰資訊(Ks)也可以基於2G鑑別向量(2G鑑別向量(AV=RAND、SRES(正負號回應)、Kc(密鑰)))。

除此之外，在依據本發明的NAF/BSF 101及UE 102中，該核心網路相關動態身分資訊(動態ID資訊)可包含一網路應用功能領域名稱伺服器(例如，NAF DNS)名稱以及/或一Ua介面協定識別符。此外，該金鑰產生相關資訊(例如，GPI)可包含一獨特使用者識別符，例如IMPI、IMPU或其他使用者識別符、至少一隨機數(RAND)或一正負號結果(SRES)、密碼金鑰內容、通用自舉架構推入資訊之以上提到的已加密部分(E_GPI)、該通用自舉架構推入資訊之一完整性保護部分(I_GPI)、導出的第一及第二金鑰、一金鑰壽命及/或至少一通用自舉架構使用者設定(GUSS)。該使用者設備處理指令資訊可包含指示(例如)Upa使用的至少一未加密資訊元件(例如，一位元)。

除此之外，依據該UE 102之進一步的實施例及細化，該UE 102之可取捨的創建器1028可被組配以基於該隨機數(RAND)及該鑑別符記(AUTN)產生通用金鑰資訊(Ks，如以虛線鑰匙符號所指示的)。此外，該UE 102之可取捨鑑別器

1029可被組配以基於該第一金鑰資訊A1'鑑別該通用自舉架構推入資訊(I_GPI)之完整性保護部分。該第一金鑰資訊A1'可以是對應由該NAF/BSF 101之產生器1015產生的金鑰資訊A1之金鑰資訊。可選擇的方式是，該接收器1023可被組配以接收一第一金鑰產生識別符，以及該產生器1025可被組配以產生也與該接收器1023接收的該金鑰產生識別符有關的第一金鑰資訊。可選擇的方式是，該第一金鑰產生識別符可被預先組配，以及該產生器1025可被進一步組配以產生也與該預先組配的金鑰產生識別符有關的第一金鑰資訊。作為一額外選擇，(例如)該UE 102之CPU 1021可被進一步組配以基於由該導出器1027導出的第二金鑰資訊B2(例如，Ks_(ext)_NAF)處理被該接收器1023接收的以上所描述的可取捨訊息(例如，Ua訊息)。

除此之外，該UE 102可選擇地由一行動設備或一通用積體電路卡組成。而且，該可取捨創建器1028也可由一可以晶片組插入該UE 102的通用積體電路卡組成(由延伸到該UE 102之功能方塊的可取捨創建器1028之功能方塊指示)。

該UE 102可進一步包含該通用積體電路卡(1028)或一安全記憶體(圖未示)以及該可取捨介面(10210)，該可取捨介面(10210)可被組配以提供該金鑰產生相關資訊中的至少一部分(例如，GPI或GPI之部分)給該通用積體電路卡或該安全記憶體。

該UE 102也可被實施為一晶片或模組。

本發明之示範性實施例也提供一系統，該系統包含依

據本發明的該NAF/BSF 101及該UE 102中的至少一者。

本發明之示範性實施例可依據以下被總結，不限於給出的技術及實施態樣細節。

對於該UE 102的NAF金鑰導出，該NAF ID需要在該等金鑰Ks_ext/int_NAF可自Ks導出之前可得。因此，後面的金鑰對於機密地保護該NAF ID並沒有用。一種用以提供該NAF ID傳輸之機密保護之可能的解決方法是使用一額外金鑰。一額外(中間)金鑰導出可被用於此目的。作為此金鑰導出之輸入，具有不同的可能性。該BSF名稱(以及指定的特定Ua-協定身分)或任何其他一般已知的(非私密資訊破解)資訊可被使用，只要其符合該NAF-ID格式(因此不需要附加至先前發出的UICC)。這表示此NAF ID符合資訊可在該UE(智慧卡或GBA_ME及GBA_U之ME)內被預先組配或者在自舉之前被傳輸/廣播，作為兩個例子。因為此金鑰導出需在BSF內被執行，所以一BSF名稱可被使用。否則，一名稱被加到該Zpn-請求訊息內。除此之外，在使用NAF-ID=BSF名稱的BSF導出的金鑰沒有被傳給該請求NAF。這提供該NAF不能夠修改(對於該GPI之完整性保護)且讀取該GPI之受保護部分的特性。在此情形下，該BSF作為一可信賴伺服器，加密需要被傳給該UE的NAF ID。該NAF無法修改此資料。具有自一IP位址解析NAF ID之能力的UE能夠檢查且匹配此資料。同時，該已加密值作為一授權符記(類似但不等於一鑑別B-TID方法，其中此形式的B-TID作為用以檢查是否涉及該UE的裝置)，該已加密值可

被UE驗證以證明該發送NAF被授權以將資訊推入給該UE。若自舉壽命在被明文包括在GPI中且被Ks_(ext)_BSF完整性保護，則當一NAF將該GPI儲存在該網路內太久(藉由在自舉之前使壽命有效)時，其允許拒絕一UE之自舉。一發送具有無效RAND AUTN的篡改GPI之NAF無法被阻止，但是自舉嘗試將失敗。一發送具有一有效(但是未被使用的)RAND AUTN的篡改GPI之NAF無法被阻止，且若該NAF不被允許作為一推入NAF，其將也不能夠完整性保護GPI，因此被該UE檢測出(該NAF將使用Zn介面請求如3GPP規格TS 33.220指定的NAF金鑰)，則這可能導致一成功的自舉。

對於正確的金鑰導出，DNS名稱及其他金鑰導出資料可能需要被安全地傳遞給使用者且在終端機及網路端被整合到金鑰導出程序內。此機制可確保被傳遞的DNS名稱之完整性保護以及確保機密性保護(隱私)。一DNS名稱之安全性對於阻止一可能的所謂網路釣魚式攻擊是重要的。此機密保護對於避免一使用者可能經由該NAF主機名稱鏈結到某一內容可能是重要的。該機制也具有以下特性：該廣播伺服器(NAF，可能在一被造訪的網路內)不能夠修改需被發送給該UE的自舉相關資料。這允許在其他國家的漫遊使用者能夠像平常一樣接收"未過濾"資訊。

依據本發明之示範性實施例的解決方法提供一種用以保護一網路初始化GBA自舉內的一些資料免於受到篡改及觀察的機制。特別是當不具有任何基本載送器網路安全(例如，在廣播模式網路中)時，該等實施例是需要的且重要的。

本發明之其他實施例也可被提供。

出於本文以上所描述的本發明之目的，應該注意到的是，一接取技術可以是一使用者可藉以接取一接取網路的任何技術。任何現在或將來的技術，例如無線區域接取網路(WLAN)、纜線網路、微波接取之世界協作(WiMAX)、藍牙、紅外線以及類似者可被使用。應進一步注意到的是，一接取網路可以是一行動台實體或其他使用者設備可連接到及/或使用由該接取網路提供的服務之任何設備、單元或裝置。此等服務尤其包括資料及/或(音訊-)可視通訊、資料下載等。

一般而言，本發明之示範性實施例也可應用於依靠一基於資料封包的傳輸方案之該等網路/終端機環境，資料可依據該基於資料封包的傳輸方案以資料封包被發送，且其等(例如)可基於網際網路協定IP。然而，該等示範性實施例不限於此，以及任何其他現在或將來的IP或行動IP(MIP)版本，或者較一般地，遵循與(M)IPv4/6類似的原理之協定也可被應用。

一使用者設備實體可以是一系統使用者可藉以自一接取網路體驗服務的任何設備、單元或裝置。

可指出，可能實施為軟體程式碼部分且使用一處理器被執行的方法步驟是軟體程式碼獨立的，且可利用任何已知或將來發展的程式語言被指定，只要由該等方法步驟定義的整體功能被保留。

一般而言，任何方法步驟適用於實施為軟體或由硬體

實施，按照所實施的功能而沒有改變本發明之示範性實施例之本質。

可能實施為一行動台內的硬體元件或網路元件或其模組的方法步驟及/或設備、單元或裝置是硬體獨立的，且可利用任何已知或將來發展的硬體技術或其等之任何混合被實施，例如金屬氧化半導體(MOS)、互補MOS(CMOS)、雙極MOS(BiMOS)、雙極CMOS(BiCMOS)、射極耦合邏輯(ECL)、電晶體-電晶體邏輯(TTL)等，利用(例如)特定應用積體電路(IC)元件(ASIC)、可現場規劃閘極陣列(FPGA)元件、複雜可規劃邏輯裝置(CPLD)元件或數位信號處理器(DSP)元件。

除此之外，可能實施為軟體元件的任何方法步驟及/或設備、單元或裝置可(例如)基於多媒體廣播多播服務(MBMS)；特別地，MBMS安全符合軟體模組可被使用。雖然安全MBMS在本文作為一例子被用於一安全服務以供描述目的，但是能夠(例如)鑑別、授權、金鑰保護及/或保護訊務的任何安全架構可被應用。

設備、單元或裝置(例如，使用者設備、BSF及NAF)可被實施為個別設備、單元或裝置，但是這並不排除它們以一分散方式實施在該系統中，只要該設備、單元或裝置之功能被保持。

此外，被用於所描述的參數、功能、訊息類型、介面及類似者(例如，BSF、GPI、Ks_(ext/int)_BSF等)的各種名稱並不意指限於任何層面，因為該等參數、功能、訊息類

型、介面及類似者可由任何適合的名稱被識別。

應該注意到的是，詞語“連接”、“耦接”或其任何變化表示兩個或多個元件之間的任何連接或耦接，不管是直接或間接的，且可包含被“連接”或“耦接”在一起的兩個元件之間存在一或多個中間元件。該等元件之間的耦接或連接可以是實體的、邏輯的或其等一組合。如本文所使用的，兩個元件可被認為藉由使用一或多個導線、纜線及/或印刷電性連接被“連接”或“耦接”在一起，以及藉由使用電磁能量，例如具有在射頻範圍、微波範圍及光學(可見及不可見)範圍內的波長之電磁能量，作為幾個非限制性及非詳盡例子。

此外，本發明之各種非限制性及示範性實施例之一些特徵可被用以提供優勢，而不需其他特徵之對應使用。這樣，以上描述應被認為僅僅是本發明之原理、教示及示範性實施例之說明，且不是其限制。

## 【圖式簡單說明】

第1圖顯示了用於依據本發明之示範性實施例的金鑰參數供應之個別方法；以及

第2圖顯示了用於依據本發明之示範性實施例的金鑰參數供應之個別裝置(例如，一使用者設備及NAF/BSF)。

## 【主要元件符號說明】

100…通訊系統
101…網路應用功能
102…使用者設備
103…自舉伺服器功能
104…接取網路
1011…中央處理單元
1011a…中央處理單元
1012…記憶體

1013…發送器

1014…接收器

1015…產生器

1016…加密器

1017…導出器

1021…CPU

1022…記憶體

1023…發送器

1024…接收器

1025…產生器

1026…解密器

1027…導出器

1028…創建器

1029…鑑別器

10210…介面

S1-1、S1-1-1、S1-2、S1-2-1、S1-3、S1-4、S2-1、S2-1-1、S2-2、S2-2-1、S2-3、S2-4、S2-5…步驟

## 五、中文發明摘要：

一種方法包括以下步驟：對一特定使用者設備，接收金鑰產生相關資訊之一查詢及使用者設備處理指令資訊；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；基於該產生的金鑰資訊加密至少核心網路相關動態身分資訊；以及發送包含至少該已加密核心網路相關動態身分資訊及該被接收的使用者設備處理指令資訊的金鑰產生相關資訊。一種包括以下步驟的方法也被描述：接收具有至少已加密核心網路相關動態身分資訊及使用者設備處理指令資訊的金鑰產生相關資訊；產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；基於該產生的第一金鑰資訊解密該被接收的已加密核心網路相關動態身分資訊；以及基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

## 六、英文發明摘要：

A method includes receiving, for a specific user equipment, an inquiry for key generation-related information, and user equipment processing instruction information, generating first key information on the received user equipment processing instruction information, encrypting at least core-network related dynamic identity information based on the generated key information, and sending the key generation-related information comprising at least the encrypted core-network related dynamic identity information and the received user equipment processing instruction information. Also described is a method that includes receiving key generation-related information that has at least encrypted core-network related dynamic identity information and user equipment processing instruction information, generating first key information on the received user equipment processing instruction information, decrypting the received encrypted core-network related dynamic identity information based on the generated first key information, and deriving second key information based on the decrypted core-network related dynamic identity information.

## 十、申請專利範圍：

1. 一種方法，包含以下步驟：

接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

加密至少核心網路相關動態身分資訊；以及

以該金鑰產生相關資訊回復該查詢，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

2. 如申請專利範圍第1項所述之方法，其中該金鑰產生相關資訊之查詢包含一GBA-PUSH-INFO通用自舉架構推入資訊(GPI)。

3. 如申請專利範圍第1項所述之方法，其中該使用者設備處理指令資訊包含一Upa使用之一指示。

4. 如申請專利範圍第1項所述之方法，其中產生該第一金鑰資訊考量一自舉伺服器功能(BSF)名稱以及指定的特定Ua協定身分。

5. 如申請專利範圍第1項所述之方法，其中該第一金鑰資訊包含Ks_(ext/int)_BSF，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱，其中加密基於該產生的Ks_(ext/int)_BSF加密該NAF DNS名稱，導致一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)。

6. 如申請專利範圍第5項所述之方法，其中該E_GPI也包含未加密資訊。
7. 如申請專利範圍第6項所述之方法，其中該未加密資訊包含Upa使用。
8. 如申請專利範圍第6項所述之方法，其中該未加密資訊包含通用積體電路卡(UICC)選擇資訊。
9. 如申請專利範圍第1項所述之方法，其中產生包含獲得一鑑別向量(AV)。
10. 如申請專利範圍第9項所述之方法，其中該AV包含密碼金鑰內容，該密碼金鑰內容包含用於產生該第一金鑰資訊的一隨機數(RAND)、一鑑別符記(AUTN)、一被期望的回應(XRES)、一密鑰(CK)以及一完整性金鑰(IK)中的至少一者。
11. 如申請專利範圍第1項所述之方法，其中該被接收的使用者設備處理指令資訊包含一行動應用識別符Ua-appli-id。
12. 如申請專利範圍第1項所述之方法，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱以及一Ua介面協定識別符中的至少一者。
13. 如申請專利範圍第1項所述之方法，其中該金鑰產生相關資訊包含一獨特使用者識別符。
14. 如申請專利範圍第1項所述之方法，其中該金鑰產生相關資訊包含一網際網路協定多媒體子系統私人使用者身分(IMPI)或一網際網路協定多媒體子系統公共使用

者身分(IMPU)。

15. 如申請專利範圍第1項所述之方法，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

16. 如申請專利範圍第1項所述之方法，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

17. 一種被組配以儲存程式指令的記憶體媒體，該等程式指令之執行導致執行包含以下步驟的操作：

接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

加密至少核心網路相關動態身分資訊；以及

以該金鑰產生相關資訊回復該查詢，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

18. 如申請專利範圍第17項所述之記憶體媒體，其中該金鑰產生相關資訊之查詢包含一GBA-PUSH-INFO通用自舉架構推入資訊(GPI)。

19. 如申請專利範圍第17項所述之記憶體媒體，其中該使用

者設備處理指令資訊包含一Upa使用之一指示。

20. 如申請專利範圍第17項所述之記憶體媒體，其中產生該第一金鑰資訊考量一自舉伺服器功能(BSF)名稱以及指定的特定-Ua協定身分。

21. 如申請專利範圍第17項所述之記憶體媒體，其中該第一金鑰資訊包含Ks_(ext/int)_BSF，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱，其中加密基於該產生的Ks_(ext/int)_BSF加密該NAF DNS名稱，導致一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)。

22. 如申請專利範圍第21項所述之記憶體媒體，其中該E_GPI也包含未加密資訊。

23. 如申請專利範圍第22項所述之記憶體媒體，其中該未加密資訊包含Upa使用。

24. 如申請專利範圍第22項所述之記憶體媒體，其中該未加密資訊包含通用積體電路卡(UICC)選擇資訊。

25. 如申請專利範圍第17項所述之記憶體媒體，其中產生包含獲得一鑑別向量(AV)。

26. 如申請專利範圍第25項所述之記憶體媒體，其中該AV包含密碼金鑰內容，該密碼金鑰內容包含一隨機數(RAND)、一鑑別符記(AUTN)、一被期望的回應(XRES)、一密鑰(CK)以及一用於產生該第一金鑰資訊的完整性金鑰(IK)中的至少一者。

27. 如申請專利範圍第17項所述之記憶體媒體，其中該被接

收的使用者設備處理指令資訊包含一行動應用識別符Ua-appli-id。

28. 如申請專利範圍第17項所述之記憶體媒體，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱以及一Ua介面協定識別符中的至少一者。

29. 如申請專利範圍第17項所述之記憶體媒體，其中該金鑰產生相關資訊包含一獨特使用者識別符。

30. 如申請專利範圍第17項所述之記憶體媒體，其中該金鑰產生相關資訊包含一網際網路協定多媒體子系統私人使用者身分(IMPI)或一網際網路協定多媒體子系統公共使用者身分(IMPU)。

31. 如申請專利範圍第17項所述之記憶體媒體，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

32. 如申請專利範圍第17項所述之記憶體媒體，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

33. 如申請專利範圍第17項所述之記憶體媒體，以一自舉伺服器功能(BSF)實施。

34. 如申請專利範圍第17項所述之記憶體媒體，以一積體電

路晶片或模組實施。

35. 一種裝置，包含：

一接收器，被組配以接收使用者設備處理指令資訊以及金鑰產生相關資訊之一請求；

一產生器，被組配以產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

一加密器，被組配以加密至少核心網路相關動態身分資訊；以及

一發送器，被組配以以該金鑰產生相關資訊回應該請求，該金鑰產生相關資訊包含至少該已加密核心網路相關動態身分資訊及被接收的使用者設備處理指令資訊。

36. 如申請專利範圍第35項所述之裝置，其中該金鑰產生相關資訊之請求包含一GBA-PUSH-INFO通用自舉架構推入資訊(GPI)。

37. 如申請專利範圍第35項所述之裝置，其中該使用者設備處理指令資訊包含一Upa使用之一指示。

38. 如申請專利範圍第35項所述之裝置，其中該產生器產生該第一金鑰資訊時考量一自舉伺服器功能(BSF)名稱以及指定的特定-Ua協定身分。

39. 如申請專利範圍第35項所述之裝置，其中該第一金鑰資訊包含Ks_(ext/int)_BSF，其中該核心網路相關動態身分資訊包含一網路應用功能域名伺服器(NAF DNS)名稱，其中加密基於該產生的Ks_(ext/int)_BSF加密該NAF DNS名稱，導致一通用自舉架構推入資訊(GPI)之一已加

密部分(E_GPI)。

40. 如申請專利範圍第39項所述之裝置，其中該E_GPI也包含未加密資訊。

41. 如申請專利範圍第39項所述之裝置，其中該未加密資訊包含Upa使用。

42. 如申請專利範圍第39項所述之裝置，其中該未加密資訊包含通用積體電路卡(UICC)選擇資訊。

43. 如申請專利範圍第35項所述之裝置，其中該產生器被進一步組配以獲得一鑑別向量(AV)。

44. 如申請專利範圍第43項所述之裝置，其中該AV包含密碼金鑰內容，該密碼金鑰內容包含一隨機數(RAND)、一鑑別符記(AUTN)、一被期望的回應(XRES)、一密鑰(CK)以及一用於產生該第一金鑰資訊的完整性金鑰(IK)中的至少一者。

45. 如申請專利範圍第35項所述之裝置，其中該被接收的使用者設備處理指令資訊包含一行動應用識別符Ua-appli-id。

46. 如申請專利範圍第35項所述之裝置，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱以及一Ua介面協定識別符中的至少一者。

47. 如申請專利範圍第35項所述之裝置，其中該金鑰產生相關資訊包含一獨特使用者識別符。

48. 如申請專利範圍第35項所述之裝置，其中該金鑰產生相關資訊包含一網際網路協定多媒體子系統私人使用者

身分(IMPI)或一網際網路協定多媒體子系統公共使用者身分(IMPU)。

49. 如申請專利範圍第35項所述之裝置，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

50. 如申請專利範圍第35項所述之裝置，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

51. 如申請專利範圍第35項所述之裝置，以一自舉伺服器功能(BSF)實施。

52. 如申請專利範圍第35項所述之裝置，以一積體電路晶片或模組實施。

53. 一種裝置，包含：

用於接收使用者設備處理指令資訊以及金鑰產生相關資訊之一查詢的裝置；

用於產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊的裝置；

用於加密至少核心網路相關動態身分資訊的裝置；以及

用於以該金鑰產生相關資訊回復該查詢的裝置，該金鑰產生相關資訊包含至少該已加密核心網路相關動

態身分資訊及被接收的使用者設備處理指令資訊。

54. 如申請專利範圍第53項所述之裝置，其中該金鑰產生相關資訊之查詢包含一GBA-PUSH-INFO通用自舉架構推入資訊(GPI)，其中該使用者設備處理指令資訊包含一Upa使用之一指示。

55. 如申請專利範圍第53項所述之裝置，其中該第一金鑰資訊包含Ks_(ext/int)_BSF，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱，其中該加密裝置基於該產生的Ks_(ext/int)_BSF加密該NAF DNS名稱，導致一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)，其中該E_GPI也包含未加密資訊。

56. 如申請專利範圍第53項所述之裝置，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱以及一Ua介面協定識別符中的至少一者。

57. 如申請專利範圍第53項所述之裝置，以與透過一基地台與該使用者設備耦接的一接取網路實施。

58. 如申請專利範圍第53項所述之裝置，以一自舉伺服器功能(BSF)實施。

59. 如申請專利範圍第53項所述之裝置，以一積體電路晶片或模組實施。

60. 一種方法，包含以下步驟：

接收使用者設備處理指令資訊以及包含至少已加

密核心網路相關動態身分資訊的金鑰產生相關資訊；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

解密該被接收的已加密核心網路相關動態身分資訊；以及

基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

61. 如申請專利範圍第60項所述之方法，其中該被接收的金鑰產生相關資訊包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)。

62. 如申請專利範圍第60項所述之方法，其中該已加密核心網路相關動態身分資訊包括一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)，該E_GPI包含一已加密網路應用功能領域名稱伺服器(NAF DNS)名稱，以及其中該使用者設備處理指令資訊包含Upa使用之一指示。

63. 如申請專利範圍第60項所述之方法，其中產生該第一金鑰資訊使用存在該使用者設備內的一通用積體電路卡(UICC)之Ks_(ext)_BSF。

64. 如申請專利範圍第60項所述之方法，其中產生該第一金鑰資訊考量一自舉伺服器功能(BSF)名稱以及指定的特定Ua-協定身分。

65. 如申請專利範圍第60項所述之方法，其中解密該被接收的已加密核心網路相關動態身分資訊基於該產生的第一金鑰資訊解密一已加密通用自舉架構推入資訊

(GPI)，導致一網路應用功能(NAF)之一DNS名稱。

66. 如申請專利範圍第60項所述之方法，其中導出第二金鑰資訊導出Ks_(ext)_NAF。

67. 如申請專利範圍第60項所述之方法，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱及一Ua介面協定識別符中的至少一者。

68. 如申請專利範圍第60項所述之方法，其中該金鑰產生相關資訊包含一獨特使用者識別符。

69. 如申請專利範圍第60項所述之方法，其中該金鑰產生相關資訊包含一網際網路協定多媒體子系統私人使用者身分(IMPI)或一網際網路多媒體子系統公共使用者身分(IMPU)。

70. 如申請專利範圍第60項所述之方法，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

71. 如申請專利範圍第60項所述之方法，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

72. 一種被組配以儲存程式指令的記憶體媒體，其之執行導致執行包含以下步驟的操作：

接收使用者設備處理指令資訊以及包含至少已加

密核心網路相關動態身分資訊的金鑰產生相關資訊；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；

解密該被接收的已加密核心網路相關動態身分資訊；以及

基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

73. 如申請專利範圍第72項所述之記憶體媒體，其中該被接收的金鑰產生相關資訊包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)。

74. 如申請專利範圍第72項所述之記憶體媒體，其中該已加密核心網路相關動態身分資訊包括一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)，該E_GPI包含一已加密網路應用功能領域名稱伺服器(NAF DNS)名稱，以及其中該使用者設備處理指令資訊包含Upa使用之一指示。

75. 如申請專利範圍第72項所述之記憶體媒體，其中產生該第一金鑰資訊使用存在該使用者設備內的一通用積體電路卡(UICC)上的Ks_(ext)_BSF。

76. 如申請專利範圍第72項所述之記憶體媒體，其中產生該第一金鑰資訊考量一自舉伺服器功能(BSF)名稱以及指定的特定Ua-協定身分。

77. 如申請專利範圍第72項所述之記憶體媒體，其中解密該被接收的已加密核心網路相關動態身分資訊基於該產

生的第一金鑰資訊解密一已加密通用自舉架構推入資訊(GPI)，導致一網路應用功能(NAF)之一DNS名稱。

78. 如申請專利範圍第72項所述之記憶體媒體，其中導出第二金鑰資訊導出Ks_(ext)_NAF。

79. 如申請專利範圍第72項所述之記憶體媒體，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱及一Ua介面協定識別符中的至少一者。

80. 如申請專利範圍第72項所述之記憶體媒體，其中該金鑰產生相關資訊包含一獨特使用者識別符。

81. 如申請專利範圍第72項所述之記憶體媒體，其中該金鑰產生相關資訊包含一網際網路協定多媒體子系統私人使用者身分(IMPI)或一網際網路多媒體子系統公共使用者身分(IMPU)。

82. 如申請專利範圍第72項所述之記憶體媒體，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

83. 如申請專利範圍第72項所述之記憶體媒體，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

84. 一種裝置，包含：

一接收器，被組配以接收使用者設備處理指令資訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊；

一產生器，被組配以產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊；以及

一解密器，被組配以解密該被接收的已加密核心網路相關動態身分資訊以用於基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊。

85. 如申請專利範圍第84項所述之裝置，其中該被接收的金鑰產生相關資訊包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)。

86. 如申請專利範圍第84項所述之裝置，其中該已加密核心網路相關動態身分資訊包括一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)，該E_GPI包含一已加密網路應用功能領域名稱伺服器(NAF DNS)名稱，以及其中該使用者設備處理指令資訊包含Upa使用之一指示。

87. 如申請專利範圍第84項所述之裝置，其中該產生器至少部分依據存在一使用者設備內的一通用積體電路卡(UICC)上的Ks_(ext)_BSF產生該第一金鑰資訊。

88. 如申請專利範圍第84項所述之裝置，其中該產生器至少部分依據一自舉伺服器功能(BSF)名稱以及指定的特定Ua-協定身分產生該第一金鑰資訊。

89. 如申請專利範圍第84項所述之裝置，其中該解密器基於該產生的第一金鑰資訊解密一已加密通用自舉架構推入

資訊(GPI)，導致一網路應用功能(NAF)之一DNS名稱。

90. 如申請專利範圍第84項所述之裝置，其中導出的第二金鑰資訊包含Ks_(ext)_NAF。

91. 如申請專利範圍第84項所述之裝置，其中該核心網路相關動態身分資訊包含一網路應用功能領域名稱伺服器(NAF DNS)名稱及一Ua介面協定識別符中的至少一者。

92. 如申請專利範圍第84項所述之裝置，其中該金鑰產生相關資訊包含一獨特使用者識別符。

93. 如申請專利範圍第84項所述之裝置，其中該金鑰產生相關資訊包含一隨機數及一正負號結果中的至少一者；密碼金鑰內容；通用自舉架構推入資訊之一已加密部分；該通用自舉架構推入資訊之一完整性保護部分；導出的第一及第二金鑰；一金鑰壽命；以及至少一通用自舉架構使用者設定。

94. 如申請專利範圍第84項所述之裝置，其中該使用者設備處理指令資訊包含指示行動性選擇的至少一未加密資訊元件。

95. 如申請專利範圍第84項所述之裝置，以一積體電路晶片或模組實施。

96. 一種裝置，包含：

用於接收使用者設備處理指令資訊以及包含至少已加密核心網路相關動態身分資訊的金鑰產生相關資訊的裝置；

用於產生與該被接收的使用者設備處理指令資訊

有關的第一金鑰資訊的裝置；

用於解密該被接收的已加密核心網路相關動態身分資訊的裝置；以及

用於基於該已解密核心網路相關動態身分資訊導出第二金鑰資訊的裝置。

97. 如申請專利範圍第96項所述之裝置，其中該被接收的金鑰產生相關資訊包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)。

98. 如申請專利範圍第96項所述之裝置，其中該已加密核心網路相關動態身分資訊包括一通用自舉架構推入資訊(GPI)之一已加密部分(E_GPI)，該E_GPI包含一已加密網路應用功能域名伺服器(NAF DNS)名稱，以及其中該使用者設備處理指令資訊包含Upa使用之一指示。

99. 如申請專利範圍第96項所述之裝置，其中該解密裝置解密一已加密通用自舉架構推入資訊(GPI)，導致一網路應用功能(NAF)之一DNS名稱，以及其中該第二金鑰資訊包含Ks_(ext)_NAF。

100. 如申請專利範圍第96項所述之裝置，其中該核心網路相關動態身分資訊包含一網路應用功能域名伺服器(NAF DNS)名稱及一Ua介面協定識別符中的至少一者，以及其中該金鑰產生相關資訊包含一獨特使用者識別符。

101. 如申請專利範圍第96項所述之裝置，以一積體電路晶片或模組實施。

102. 如申請專利範圍第96項所述之裝置，其中該用於解密的

裝置進一步用於基於該產生的第一金鑰資訊解密該被接收的已加密核心網路相關動態身分資訊。

103.一種方法，包含以下步驟：

接收使用者設備處理指令資訊以及一通用自舉架構推入資訊(GPI)之一查詢；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊(Ks_(ext/int)_BSF)；

加密至少一網路應用功能域名伺服器(NAF DNS)名稱，其中該GPI之一E_GPI部分包含該已加密NAF DNS名稱；以及

以該E_GPI及被接收的使用者設備處理指令資訊答復該查詢。

104.一種方法，包含以下步驟：

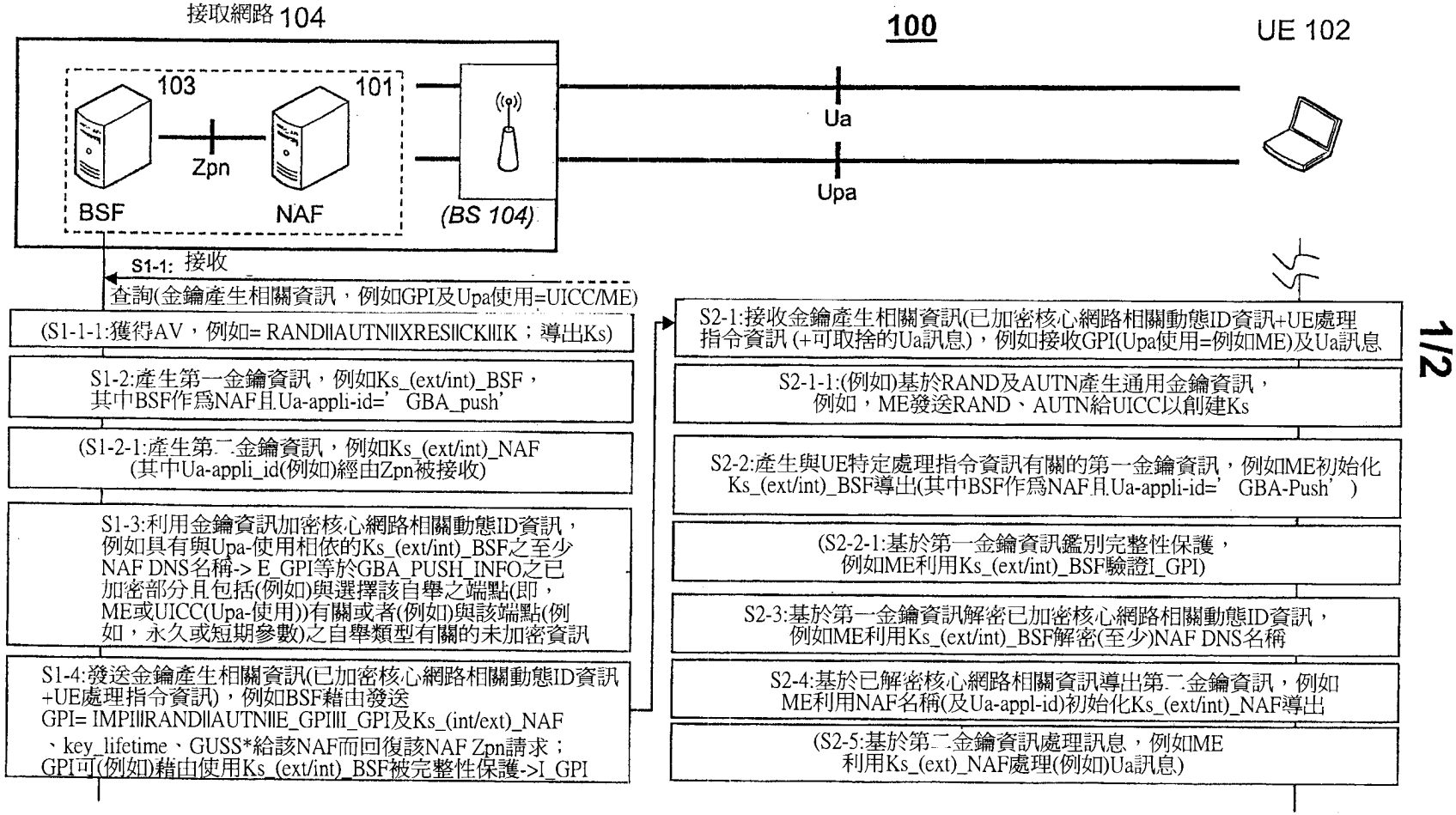
接收一訊息，該訊息包含由一網路應用功能(NAF)推入的一通用自舉架構推入資訊(GPI)以及使用者設備處理指令資訊，其中該GPI之一E_GPI部分包含一已加密網路應用功能領域名稱伺服器(NAF DNS)名稱；

產生與該被接收的使用者設備處理指令資訊有關的第一金鑰資訊(Ks_(ext/int)_BSF)；

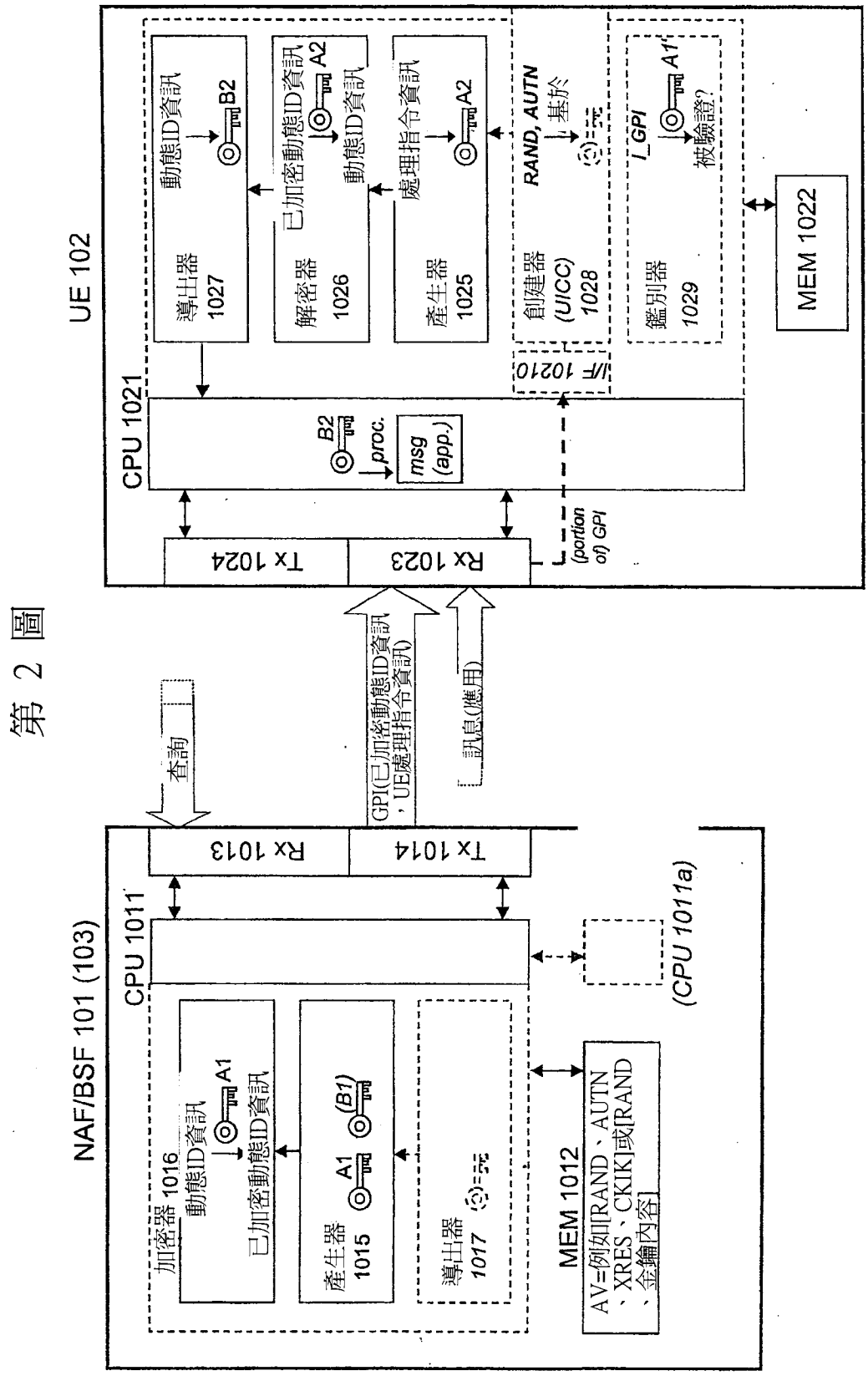
解密該被接收的已加密NAF DNS名稱；以及

基於該已解密NAF DNS名稱導出第二金鑰資訊(Ks_(ext/int)_NAF)。

# 第 1 圖


接取網路 104
100
UE 102
103
101
Zpn
BSF
NAF
(BS 104)
Ua
Upa
S1-1: 接收
查詢(金鑰產生相關資訊，例如GPI及Upa使用=UICC/ME)
(S1-1-1:獲得AV，例如= RAND||AUTN||XRES||CK||IK；導出Ks)
S1-2:產生第一金鑰資訊，例如Ks_(ext/int)_BSF，其中BSF作爲NAF且Ua-appli-id=' GBA_push'
(S1-2-1:產生第二金鑰資訊，例如Ks_(ext/int)_NAF (其中Ua-appli_id(例如)經由Zpn被接收)
S1-3:利用金鑰資訊加密核心網路相關動態ID資訊，例如具有與Upa-使用相依的Ks_(ext/int)_BSF之至少NAF DNS名稱-> E_GPI等於GBA_PUSH_INFO之已加密部分且包括(例如)與選擇該自舉之端點(即，ME或UICC(Upa-使用))有關或者(例如)與該端點(例如，永久或短期參數)之自舉類型有關的未加密資訊
S1-4:發送金鑰產生相關資訊(已加密核心網路相關動態ID資訊+UE處理指令資訊)，例如BSF藉由發送GPI= IMPI||RAND||AUTN||E_GPI||I_GPI及Ks_(int/ext)_NAF、key_lifetime、GUSS*給該NAF而回復該NAF Zpn請求；GPI可(例如)藉由使用Ks_(ext/int)_BSF被完整性保護->I_GPI
S2-1:接收金鑰產生相關資訊(已加密核心網路相關動態ID資訊+UE處理指令資訊 (+可取捨的Ua訊息)，例如接收GPI(Upa使用=例如ME)及Ua訊息
S2-1-1:(例如)基於RAND及AUTN產生通用金鑰資訊，例如，ME發送RAND、AUTN給UICC以創建Ks
S2-2:產生與UE特定處理指令資訊有關的第一金鑰資訊，例如ME初始化Ks_(ext/int)_BSF導出(其中BSF作爲NAF且Ua-appli-id=' GBA-Push' )
(S2-2-1:基於第一金鑰資訊鑑別完整性保護，例如ME利用Ks_(ext/int)_BSF驗證I_GPI)
S2-3:基於第一金鑰資訊解密已加密核心網路相關動態ID資訊，例如ME利用Ks_(ext/int)_BSF解密(至少)NAF DNS名稱
S2-4:基於已解密核心網路相關資訊導出第二金鑰資訊，例如ME利用NAF名稱(及Ua-appl-id)初始化Ks_(ext/int)_NAF導出
(S2-5:基於第二金鑰資訊處理訊息，例如ME利用Ks_(ext)_NAF處理(例如)Ua訊息)

第 2 圖


UE 102
CPU 1021
導出器 1027
動態ID資訊
B2
解密器 1026
已加密動態ID資訊
A2
動態ID資訊
產生器 1025
處理指令資訊
A2
創建器 (UICC) 1028
RAND, AUTN
基於
I/F 10210
鑑別器 1029
I_GPI
A1
被驗證?
MEM 1022
B2
proc.
msg (app.)
(portion of) GPI
Tx 1024
Rx 1023
GPI(已加密動態ID資訊，UE處理指令資訊)
訊息(應用)
查詢
NAF/BSF 101 (103)
CPU 1011
加密器 1016
動態ID資訊
A1
已加密動態ID資訊
產生器 1015
A1
(B1)
導出器 1017
MEM 1012
AV=例如[RAND、AUTN、XRES、CKIK]或[RAND、金鑰內容]
(CPU 1011a)
Tx 1014
Rx 1013

## 七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100…通訊系統
101…網路應用功能
102…使用者設備
103…自舉伺服器功能
104…接取網路

S1-1、S1-1-1、S1-2、S1-2-1、S1-3、S1-4、S2-1、S2-1-1、S2-2、S2-2-1、S2-3、S2-4、S2-5…步驟

## 八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

200915814

双面影印

# 發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

97.12.13 修正補充

**※ 申請案號：** 97125032

**※ 申請日期：** **※IPC 分類：** H04L 9/08 (2006.01) H04L 9/12 (2006.01)

## 一、發明名稱：（中文/英文）

用於金鑰參數供應的方法、裝置、系統、與電腦程式

METHOD, APPARATUS, SYSTEM AND COMPUTER PROGRAM FOR KEY PARAMETER PROVISIONING

## 二、申請人：（共 1 人）

**姓名或名稱：**（中文/英文）

諾基亞西門子通信股份有限公司 / NOKIA SIEMENS NETWORKS OY

**代表人：**（中文/英文）

波格斯壯　馬克思 / BORGSTROM, MARKUS

**住居所或營業所地址：**（中文/英文）

芬蘭艾斯浦・卡拉波堤 3 號

Karaportti 3, 02610 Espoo, Finland

**國　籍：**（中文/英文）

芬蘭 / FINLAND

## 三、發明人：（共 2 人）

**姓　名：**（中文/英文）

1. 布隆馬特　馬克 / BLOMMAERT, MARC
2. 荷特曼斯　西爾克 / HOLTMANNS, SILKE

**國　籍：**（中文/英文）

1. 比利時 / BELGIUM
2. 丹麥 / DENMARK

## 四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 美國、　2007/07/03、　60/929,589

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。