I796819

(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I796819 B

(45)公告日： 中華民國 112 (2023) 年 03 月 21 日

(21)申請案號：110140276 (22)申請日： 中華民國 110 (2021) 年 10 月 29 日

(51)Int. Cl.： *H04L9/06 (2006.01)* *H04L9/08 (2006.01)*

(30)優先權：2020/10/30 美國 63/108,082

2021/10/26 世界智慧財產權組織 PCT/EP2021/079700

(71)申請人：瑞典商ＬＭ艾瑞克生(ＰＵＢＬ)電話公司 (瑞典) TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)

瑞典

(72)發明人：威弗森 莫妮卡 WIFVESSON, MONICA (SE)；付璋 FU, ZHANG (CN)；雷托維塔 維莎 LEHTOVIRTA, VESA (FI)

(74)代理人：蔣大中

(56)參考文獻：

TW 201947980A US 10694427B2

期刊 3GPP, "3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of enhancement for proximity based services in the 5G System (5GS)(Release 17)", 3GPP Technical Report, TR 33.847 V0.2.0 (2020-10), 3GPP, 2020/10/26. https://www.3gpp.org/ftp//Specs/archive/33_series/33.847/33847-020.zip

審查人員：黃偉倫

申請專利範圍項數：36 項 圖式數：10 共 63 頁

(54)名稱

處理通信裝置-網路中繼場景中之密鑰管理之應用功能

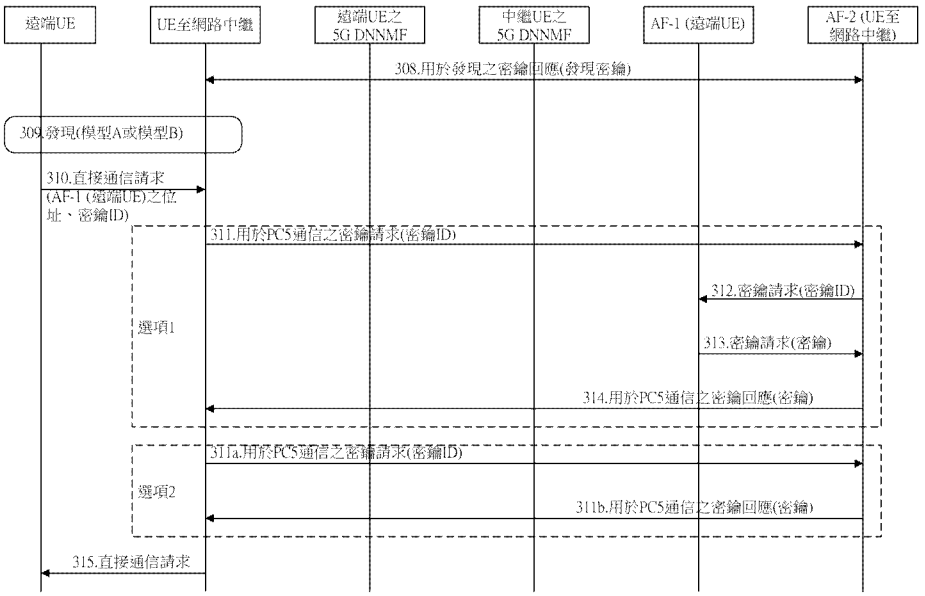
(57)摘要

一種遠端通信裝置可接收一發現密鑰；接收一通信密鑰及用於該通信密鑰之一密鑰識別符 ID；及發現一中繼通信裝置。發現該中繼通信裝置可包含從該中繼通信裝置接收一經加密發現訊息，且使用該發現密鑰解密該經加密發現訊息。該遠端通信裝置可進一步回應於接收及解密來自該中繼通信裝置之該經加密發現訊息而將一直接通信請求傳輸至該中繼通信裝置。該直接通信請求可包含用於該通信密鑰之該密鑰 ID。該遠端通信裝置可進一步從該中繼通信裝置接收一經加密直接通信回應。接收該經加密直接通信回應可包含解密該經加密直接通信回應。

A remote communication device can receive a discovery key; receive a communication key and a key identifier, ID, for the communication key; and discover a relay communication device. Discovering the relay communication device can include receiving an encrypted discovery message from the relay communication device and decrypting the encrypted discovery message using the discovery key. The remote communication device can further transmit a direct communication request to the relay communication device responsive to receiving and decrypting the encrypted discovery message from the relay communication device. The direct communication request can include the key ID for the communication key. The remote communication device can further receive an encrypted direct communication response from the relay communication

device. Receiving the encrypted direct communication response can include decrypting the encrypted direct communication response.

指定代表圖：



【圖3B】

符號簡單說明：

308:操作

309:操作

310:操作

311:操作

311a:操作

311b:操作

312:操作

313:操作

314:操作

315:操作

公告本

I796819

【發明摘要】

【中文發明名稱】

處理通信裝置-網路中繼場景中之密鑰管理之應用功能

【英文發明名稱】

HANDLING APPLICATION FUNCTIONS FOR KEY MANAGEMENT IN COMMUNICATION DEVICE-NETWORK RELAY SCENARIOS

【中文】

一種遠端通信裝置可接收一發現密鑰；接收一通信密鑰及用於該通信密鑰之一密鑰識別符ID；及發現一中繼通信裝置。發現該中繼通信裝置可包含從該中繼通信裝置接收一經加密發現訊息，且使用該發現密鑰解密該經加密發現訊息。該遠端通信裝置可進一步回應於接收及解密來自該中繼通信裝置之該經加密發現訊息而將一直接通信請求傳輸至該中繼通信裝置。該直接通信請求可包含用於該通信密鑰之該密鑰ID。該遠端通信裝置可進一步從該中繼通信裝置接收一經加密直接通信回應。接收該經加密直接通信回應可包含解密該經加密直接通信回應。

【英文】

A remote communication device can receive a discovery key; receive a communication key and a key identifier, ID, for the communication key; and discover a relay communication device. Discovering the relay communication device can include receiving an encrypted discovery message from the relay communication device and decrypting the encrypted discovery message using the discovery key.

The remote communication device can further transmit a direct communication request to the relay communication device responsive to receiving and decrypting the encrypted discovery message from the relay communication device. The direct communication request can include the key ID for the communication key. The remote communication device can further receive an encrypted direct communication response from the relay communication device. Receiving the encrypted direct communication response can include decrypting the encrypted direct communication response.

【指定代表圖】

圖3B

【代表圖之符號簡單說明】

308: 操作

309: 操作

310: 操作

311: 操作

311a: 操作

311b: 操作

312: 操作

313: 操作

314: 操作

315: 操作

【發明說明書】

【中文發明名稱】

處理通信裝置-網路中繼場景中之密鑰管理之應用功能

【英文發明名稱】

HANDLING APPLICATION FUNCTIONS FOR KEY MANAGEMENT IN COMMUNICATION DEVICE-NETWORK RELAY SCENARIOS

【技術領域】

【0001】 本發明大體上係關於通信，且更特定言之係關於支援無線通信之通信方法及相關裝置及節點。

【先前技術】

【0002】 下文描述第四代(「4G」)系統中之近接服務(「ProSe」)。一4G系統中之一ProSe使用者設備(「UE」)至網路中繼程序可包含兩個相異階段：一發現階段(例如，一UE至網路中繼之發現)及一通信階段(例如，一遠端UE與UE至網路中繼之間的通信)。一遠端UE與一UE至網路中繼之間的通信之安全性可使用用以建置安全內容脈絡且保護實際通信之一程序。特定於UE至網路中繼使用案例之安全建置之部分係共用密鑰密鑰分配器(「KD」)之建置。圖1係繪示一UE至網路中繼安全程序中之操作之一信號流程圖。

【0003】 按照用於公共安全一對一通信的流程之一般序列，可需要建置一共用密鑰KD。此密鑰可用於導出遠端UE與UE至網路中繼之間的工作階段密鑰。

【0004】 為了產生KD，遠端UE可需要來自一ProSe密鑰管理功能

(「PKMF」)之一ProSe中繼使用者密鑰(「PRUK」)及一相關聯64位元PRUK識別符(「ID」)。PRUK ID可用於識別UE至網路中繼之PKMF之PRUK。PRUK可用於在一特定PKMF下針對任何中繼產生共用密鑰KD。因此，可需要來自一特定PKMF之各遠端UE之僅一個PRUK。此PRUK需要在其仍在覆蓋範圍內時由遠端UE提取。此暗示遠端UE必須聯繫其希望能夠使用之任何潛在中繼之全部PKMF。

【0005】 遠端UE可使用一密鑰請求/回應訊息從PKMF提取其PRUK，或可透過一通用自舉架構(「GBA」)推送功能接收其PRUK作為與中繼建置通信之部分。UE至網路中繼可藉由將PRUK ID或國際行動用戶識別(「IMSI」) (例如，若遠端UE不具有用於中繼之一PRUK或所供應之PRUK已被拒絕)發送至其PKMF來提取將用於保全通信之KD。在PKMF側處，擷取對應PRUK。接著，使用一KD新鮮度參數(一本端產生之隨機數)(PKMF接著經由UE至網路中繼將其傳遞至遠端UE)、由遠端UE經由UE至網路中繼發送之一次性碼及遠端UE希望存取之中繼服務碼從PRUK導出KD。UE至網路中繼接收KD及KD新鮮度參數，且儲存KD。在已獲得KD新鮮度參數的情況下，UE至網路中繼使遠端UE能夠導出與由PKMF導出之KD相同之KD。

【0006】 若遠端UE在一密鑰回應訊息中接收到一新PRUK，則其可刪除該PKMF之任何先前PRUK。若其透過一GBA PUSH訊息接收一新PRUK，則其可覆寫透過一GBA PUSH訊息接收之尚未成功用於建置一中繼連接之任何PRUK。一旦透過一GBA PUSH訊息接收之一PRUK已用於計算一成功中繼連接建置之一KD，遠端UE便可刪除此PKMF之任何先前PRUK。

【0007】 下文描述一第五代(「5G」)系統中之ProSe之一UE中之組態。基於使用者平面之架構提出將ProSe功能之功能採用至5G系統架構中。在一些實例中，一ProSe功能之直接發現名稱管理功能(「DDNMF」)及直接佈建功能(「DPF」)對於支援5G系統架構中之ProSe可為有用/必要的。一DPF可用於向UE佈建必要參數，以便使用5G ProSe直接發現及5G Prose直接通信，其等可由一策略控制功能(「PCF」)取代。DDNMF可用於經由一PC3介面提供以下程序：一發現請求/回應程序；一匹配報告程序；一通告警報程序；及/或一發現更新程序。

【0008】 一發現請求/回應程序可為直接發現提供ID及濾波器。一匹配報告程序可檢查直接發現且為直接發現提供映射資訊。在ProSe限制發現模型A之情況中，一通告警報程序可支援「隨選」ProSe直接發現。一發現更新程序可更新/撤銷先前分配之ID、濾波器。

【0009】 5G系統(「5GS」)可支援基於服務之架構(「SBA」)，且DDNMF可為一網路功能(「NF」)，其不僅能夠與5G NF互動(例如，以消耗Nudm服務操作)，而且針對一功率分類3 (「PC3」)介面上的支援程序經由使用者平面連接性與一UE連接。在架構中，提出引入5G DDNMF，如圖2中展示，其繪示用於ProSe之所提出5G系統架構。

【0010】 5G DDNMF可由一行動網路營運商(「MNO」)管理。5G DDNMF可消耗來自5GC中之其他NF (例如，Nudm或Npcf)之服務操作。

【0011】 一PC3介面可支援一發現請求/回應、一匹配報告程序、一通告警報程序及一發現更新程序作為以下基線特徵。哪一網路切片選擇輔助資訊(「NSSAI」)或資料網路名稱(「DNN」)待用於針對一PC3介面之使用者平面連接性取決於一MNO之組態(例如，其可由一UE路由選擇策

略(「URSP」)或UE中之本端組態來控制)。

【0012】下文描述一UE至網路中繼。第三代合作夥伴計劃(「3GPP」)尚未判定針對5GS中之UE至網路中繼之一解決方案。在4G(演進封包系統(「EPS」))中，一UE至網路中繼之使用案例僅用於公共安全。但在5GS中，UE至網路中繼適用於公共安全及商業使用案例兩者。

【發明內容】

【0013】根據一些實施例，提供一種操作一遠端通信裝置之方法。該方法包含接收一發現密鑰。該方法進一步包含接收一通信密鑰及用於該通信密鑰之一密鑰識別符ID。該方法進一步包含發現一中繼通信裝置。發現該中繼通信裝置包含從該中繼通信裝置接收一經加密發現訊息，且使用該發現密鑰解密該經加密發現訊息。該方法進一步包含回應於接收及解密來自該中繼通信裝置之該經加密發現訊息而將一直接通信請求傳輸至該中繼通信裝置。該直接通信請求包含用於該通信密鑰之該密鑰ID。該方法進一步包含從該中繼通信裝置接收一經加密直接通信回應。接收該經加密直接通信回應包含解密該經加密直接通信回應。

【0014】根據其他實施例，提供一種操作一中繼通信裝置之方法。該方法包含接收一發現密鑰。該方法進一步包含傳輸一經加密發現訊息。使用該發現密鑰加密該經加密發現訊息。該方法進一步包含從一遠端通信裝置接收一直接通信請求。該直接通信請求包含一密鑰ID。該方法進一步包含獲得對應於來自該直接通信請求之該密鑰ID之一通信密鑰。該方法進一步包含將一經加密直接通信回應傳輸至該遠端通信裝置。使用對應於該密鑰ID之該通信密鑰加密該經加密直接通信回應。

【0015】根據其他實施例，提供一種操作與一遠端通信裝置相關聯

之一應用功能節點(AF-1)之方法。該方法包含從該遠端通信裝置接收用於發現之一密鑰請求訊息。該密鑰請求訊息包含一中繼服務碼。該方法進一步包含基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得一發現密鑰。該方法進一步包含將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸至該遠端通信裝置。

【0016】 根據其他實施例，提供一種操作與一中繼通信裝置相關聯之一應用功能節點(AF-2)之方法。該方法包含從該中繼通信裝置接收用於發現之一密鑰請求訊息。該密鑰請求訊息包含一中繼服務碼。該方法進一步包含基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得一發現密鑰。該方法進一步包含將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸至該中繼通信裝置。

【0017】 根據其他實施例，提供及組態一種實體(例如，遠端通信裝置、一中繼通信裝置、一應用功能節點(例如，AF-1或AF-2)、一電腦程式或電腦程式碼)以執行上文方法之至少一者。

【0018】 本文中之各種實施例容許一遠端UE與一UE至網路中繼通信以擷取用於一特定中繼服務碼之發現密鑰且擷取用於PC5通信之密鑰。

【圖式簡單說明】

【0019】 經包含以提供本發明之一進一步理解且併入於本申請案中並構成本申請案之一部分之隨附圖式繪示發明概念之特定非限制性實施例。在圖式中：

【0020】 圖1係繪示UE至網路中繼安全流程之一訊息圖；

【0021】 圖2係繪示用於ProSe之一所提出5G架構之一方塊圖；

【0022】 圖3A及圖3B係繪示根據發明概念之一些實施例之用於密

鑰管理之應用功能之處理之訊息圖；

【0023】 圖4係繪示根據發明概念之一些實施例之一無線裝置UE之一方塊圖；

【0024】 圖5係繪示根據發明概念之一些實施例之一無線電存取網路RAN節點(例如，一基地台eNB/gNB)之一方塊圖；

【0025】 圖6係繪示根據發明概念之一些實施例之一核心網路CN節點(例如，一AMF節點、一SMF節點等)之一方塊圖；

【0026】 圖7至圖8係繪示根據發明概念之一些實施例之通信裝置(例如，分別為一遠端通信裝置及一中繼通信裝置)之操作之流程圖；及

【0027】 圖9至圖10係繪示根據發明概念之一些實施例之應用功能之操作之流程圖。

【實施方式】

【0028】 現將參考隨附圖式在下文中更充分描述發明概念，其中展示發明概念之實施例之實例。然而，發明概念可以許多不同形式體現且不應被解釋為限於本文中闡述之實施例。實情係，此等實施例經提供使得本發明將為透徹及完整的，且將向熟習此項技術者充分傳達本發明概念之範疇。亦應注意，此等實施例並不相互排斥。來自一項實施例之組件可默認地假定為在另一實施例中存在/使用。

【0029】 以下描述呈現所揭示標的物之各種實施例。此等實施例被呈現為教示實例且不應被解釋為限制所揭示標的物之範疇。例如，在不脫離所描述標的物之範疇的情況下，可修改、省略或擴充所描述實施例之某些細節。

【0030】 圖4係繪示根據發明概念之實施例之經組態以提供無線通

信之一通信裝置UE 400 (亦被稱為一行動終端、一行動通信終端、一無線裝置、一無線通信裝置、一無線終端、行動裝置、一無線通信終端、使用者設備(UE)、一使用者設備節點/終端/裝置等)之元件之一方塊圖。如展示，通信裝置UE可包含一天線407及收發器電路401 (亦被稱為一收發器)，該收發器電路401包含經組態以提供與一無線電存取網路之一(若干)基地台(亦被稱為一RAN節點)之上行鏈路及下行鏈路無線電通信之一傳輸器及一接收器。通信裝置UE亦可包含耦合至收發器電路之處理電路403(亦被稱為一處理器)及耦合至處理電路之記憶體電路405 (亦被稱為記憶體)。記憶體電路405可包含當由處理電路403執行時導致處理電路執行根據本文中揭示之實施例之操作之電腦可讀程式碼。根據其他實施例，處理電路403可被定義為包含記憶體，使得無需分開的記憶體電路。通信裝置UE亦可包含與處理電路403耦合之一介面(諸如一使用者介面)，及/或通信裝置UE可被併入一車輛中。

【0031】 如本文中論述，通信裝置UE之操作可由處理電路403及/或收發器電路401執行。例如，處理電路403可控制收發器電路401以透過收發器電路401在一無線電介面上將通信傳輸至一無線電存取網路節點(亦被稱為一基地台)及/或透過收發器電路401在一無線電介面上從一RAN節點接收通信。再者，模組可儲存於記憶體電路405中，且此等模組可提供指令，使得當一模組之指令由處理電路403執行時，處理電路403執行各自操作(例如，下文關於與無線通信裝置相關之實例實施例論述之操作)。根據一些實施例，一通信裝置UE 400及/或其之一(若干)元件/(若干)功能可體現為一或多個虛擬節點及/或一或多個虛擬機。

【0032】 圖5係繪示根據發明概念之實施例之經組態以提供蜂巢式

通信之一無線電存取網路(RAN)之一無線電存取網路RAN節點500 (亦被稱為一網路節點、基地台、eNodeB/eNB、gNodeB/gNB等)之元件之一方塊圖。如展示，RAN節點可包含收發器電路501 (亦被稱為一收發器)，該收發器電路501包含經組態以提供與行動終端之上行鏈路及下行鏈路無線電通信之一傳輸器及一接收器。RAN節點可包含經組態以提供與RAN及/或核心網路CN之其他節點(例如，與其他基地台)之通信之網路介面電路507 (亦被稱為一網路介面)。網路節點亦可包含耦合至收發器電路之處理電路503 (亦被稱為一處理器)及耦合至處理電路之記憶體電路505 (亦被稱為記憶體)。記憶體電路505可包含當由處理電路503執行時導致處理電路執行根據本文中揭示之實施例之操作之電腦可讀程式碼。根據其他實施例，處理電路503可被定義為包含記憶體，使得無需一分開的記憶體電路。

【0033】 如本文中論述，RAN節點之操作可由處理電路503、網路介面507及/或收發器501執行。例如，處理電路503可控制收發器501以透過收發器501在一無線電介面上將下行鏈路通信傳輸至一或多個行動終端UE及/或透過收發器501在一無線電介面上從一或多個行動終端UE接收上行鏈路通信。類似地，處理電路503可控制網路介面507以透過網路介面507將通信傳輸至一或多個其他網路節點及/或透過網路介面從一或多個其他網路節點接收通信。再者，模組可儲存於記憶體505中，且此等模組可提供指令，使得當由處理電路503執行一模組之指令時，處理電路503執行各自操作(例如，下文關於與RAN節點有關之實例實施例論述之操作)。根據一些實施例，RAN節點500及/或其之一(若干)元件/(若干)功能可體現為一或多個虛擬節點及/或一或多個虛擬機。

【0034】 根據一些其他實施例，一網路節點可被實施為不具有一收發器之一核心網路CN節點。在此等實施例中，至一無線通信裝置UE之傳輸可由網路節點起始，使得透過包含一收發器之一網路節點(例如，透過一基地台或RAN節點)提供至無線通信裝置UE之傳輸。根據其中網路節點係包含一收發器之一RAN節點之實施例，起始傳輸可包含透過收發器進行傳輸。

【0035】 圖6係繪示根據發明概念之實施例之經組態以提供蜂巢式通信之一通信網路之一核心網路CN節點(例如，一SMF節點、一AMF節點等)之元件之一方塊圖。如展示，CN節點可包含經組態以提供與核心網路及/或無線電存取網路RAN之其他節點之通信之網路介面電路607 (亦被稱為一網路節點)。CN節點亦可包含耦合至網路介面電路之一處理電路603(亦被稱為一處理器)及耦合至處理電路之記憶體電路605 (亦被稱為記憶體)。記憶體電路605可包含當由處理電路603執行時導致處理電路執行根據本文中揭示之實施例之操作之電腦可讀程式碼。根據其他實施例，處理電路603可被定義為包含記憶體，使得無需一分開的記憶體電路。

【0036】 如本文中論述，CN節點之操作可由處理電路603及/或網路介面電路607執行。例如，處理電路603可控制網路介面電路607以透過網路介面電路607將通信傳輸至一或多個其他網路節點及/或透過網路介面電路從一或多個其他網路節點接收通信。再者，模組可儲存於記憶體605中，且此等模組可提供指令，使得當由處理電路603執行一模組之指令時，處理電路603執行各自操作(例如，下文關於與核心網路節點有關之實例實施例論述之操作)。根據一些實施例，CN節點600及/或其之一(若干)元件/(若干)功能可體現為一或多個虛擬節點及/或一或多個虛擬機。

【0037】 在一些實施例中，一UE、RAN節點及/或CE節點可被稱為一實體(例如，一網路實體)。

【0038】 在4GS中，僅針對公共安全服務定義一遠端UE使用一PC5介面經由一UE至網路中繼存取一3GPP網路之場景。商業服務從不在4GS之範疇內。

【0039】 在5GS中，針對公共安全及商業服務兩者定義UE至網路中繼。

【0040】 在5GS中，針對商業服務，遠端UE事先不知道其可在其附近找到哪一UE至網路中繼。未針對商業服務描述遠端UE及UE至網路中繼如何在一PC5介面上擷取用於發現一UE至網路中繼之共同安全密鑰，及UE如何在一PC5介面上擷取用於與一UE至網路中繼之PC5通信之共同安全密鑰。

【0041】 根據發明概念之一些實施例，提供用於商業服務之一方法。在此等實施例中，遠端UE及UE至網路中繼事先不知道彼此。

【0042】 根據發明概念之一些實施例，遠端UE及UE至網路中繼找到(若干)密鑰管理伺服器((若干)AF)之位址以能夠發現彼此且在一PC5介面上通信。

【0043】 根據發明概念之一些實施例，遠端UE在其本籍PLMN中具有一相關聯AF (圖3A至圖3B中之AF-1)以進行ProSe密鑰管理。UE至網路中繼在其本籍PLMN中具有一相關聯AF (圖3A至圖3B中之AF-2)以進行ProSe密鑰管理。此兩個AF (圖3A至圖3B中之AF-1及AF-2)可定位於同一或不同PLMN中，且可彼此通信。在一些實例中，AF (AF-1及/或AF-2)之一或多者可包含一PKMF。

【0044】 根據發明概念之一些實施例，遠端UE從遠端UE之本籍5G DNNMF獲得其本籍PLMN (AF-1 (遠端UE))中之AF之中繼服務碼及位址。

【0045】 根據發明概念之一些實施例，UE至網路中繼從UE至網路中繼之本籍5G DNNMF獲得其本籍PLMN (AF-2 (UE至網路中繼))中之AF之位址。

【0046】 根據發明概念之一些實施例，UE藉由存取連接至AF2 (UE至網路中繼)之AF-1 (遠端UE)來擷取對應於中繼服務碼之發現密鑰，該AF-2經由AF-1 (遠端UE)將對應於中繼服務碼之發現密鑰提供至UE。

【0047】 根據發明概念之一些實施例，作為一選項，全部AF (例如，AF-1 (遠端UE)、AF-2 (UE至網路中繼)、AF-3等)可共用同一演算法以針對同一中繼服務碼產生發現密鑰。

【0048】 根據發明概念之一些實施例，當遠端UE已發現其附近之一UE至網路中繼時，其在PC5介面上將AF-1 (遠端UE)之位址顯式地發送至UE至網路中繼，或在PC5介面上發送之遠端UE資訊(例如，如TR 23.752參考[4]中之解決方案#6中描述)中包含AF-1 (遠端UE)之位址。

【0049】 根據發明概念之一些實施例，UE至網路中繼經由AF-2 (UE至網路中繼)聯繫AF-1 (遠端UE) (如圖3A中之選項1中描述)，或UE至網路中繼直接聯繫AF-1 (遠端UE)(如圖3B中之選項2中描述)。

【0050】 根據發明概念之一些實施例，AF-1 (遠端UE)可與AF-2 (UE至網路中繼)通信以擷取用於一特定中繼服務碼之發現密鑰。

【0051】 根據發明概念之一些實施例，一選項可為全部AF (例如，AF-1 (遠端UE)及AF-2 (UE至網路中繼)及(若干)其他AF)可共用同一演算

法以針對同一中繼服務碼產生發現密鑰。

【0052】 根據發明概念之一些實施例，AF-2 (UE至網路中繼)可與AF-1 (遠端UE)通信以擷取用於PC5通信之發現密鑰。

【0053】 根據發明概念之一些實施例，遠端UE可在一PC5介面上將AF-1 (遠端UE)位址提供至UE至網路中繼。

【0054】 根據發明概念之一些實施例，遠端UE可將AF-1 (遠端UE)之位址包含至TR 23.752[xx]中之解決方案#6中定義之遠端UE資訊參數中。AF-2 (UE至網路中繼)可藉由查看在PC5介面上從遠端UE接收之遠端UE資訊參數來找出AF-1 (遠端UE)之位址。

【0055】 圖3A及圖3B提供繪示根據發明概念之一些實施例之用於df管理之AF處理之一訊息圖。下文論述圖3A至圖3B之操作。雖然圖3A至圖3B中未明確展示，但遠端UE及UE至網路中繼之各者可被提供為根據圖4之結構之一通信裝置。因此，遠端UE與UE至網路中繼之間的通信可在一無線無線電介面上(透過各自收發器401)提供；遠端UE與各自網路節點(例如，遠端UE之5G DNNFM及/或AF-1)之間的通信可透過收發器401及一RAN節點(未展示)在一無線無線電介面上提供，且UE至網路中繼與各自網路節點(例如，中繼UE之5G DNNFM、AF-1及/或AF-2)之間的通信可透過收發器401及一RAN節點(未展示)在一無線無線電介面上提供。再者，可透過各自網路介面提供各自網路節點之間(例如，AF-1與AF-2之間)的通信。

【0056】 在操作300a，遠端UE (亦被稱為一遠端通信裝置)聯繫其本籍PLMN中之5G DNNMF以擷取定位於其本籍公共陸地行動網路PLMN中之用於ProSe密鑰管理之AF-1 (遠端UE)之位址。類似地，UE至網路中

繼(亦被稱為一中繼UE或一中繼通信裝置)聯繫其本籍PLMN中之5G DNNMF以擷取定位於其本籍PLMN中之用於ProSe密鑰管理之AF-2 (UE至網路中繼)之位址。操作300a (針對遠端UE)可在操作301之用於發現之密鑰請求之前的任何時間發生，且操作300b (UE至網路中繼)可在操作307之用於發現之密鑰請求之前的任何時間發生。

【0057】 如本文中使用，應用功能一AF-1可為由遠端UE使用之一PLMN之一密鑰管理伺服器，且應用功能二AF-2可為由UE至網路中繼使用之一PLMN之一密鑰管理伺服器。再者，UE至網路中繼可為提供與中繼服務碼相關聯之一UE至網路中繼服務之一UE。

【0058】 在操作301，遠端UE使用AF-1 (遠端UE)之位址，且藉由起始包含中繼服務碼之用於發現之一密鑰請求訊息(亦被稱為用於發現之一密鑰請求，如圖3A中展示)來聯繫AF-1 (遠端UE)。因此，遠端UE基於來自操作300a之AF-1之位址將用於發現之密鑰請求訊息傳輸至AF-1。

【0059】 在操作302，AF-1 (遠端UE)聯繫AF-2 (UE至網路中繼)且轉發包含中繼服務碼之密鑰請求訊息(亦被稱為一密鑰請求，如圖3A中展示)。AF-1可根據及/或基於中繼服務碼(例如，中繼服務碼及AF位址(或FQDN)之間的一映射)來判定AF-2之一位址。替代地，AF-1可從AF-1之PLMN之5G DDNMF獲得AF-2之位址。

【0060】 一選項可為AF-1 (遠端UE)及AF-2 (UE至網路中繼)及(若干)其他AF可共用同一演算法以針對同一中繼服務碼產生發現密鑰。此將暗示AF-1 (遠端UE)從中繼服務碼產生發現密鑰，且無需聯繫AF-2 (UE至網路中繼)來獲得發現密鑰。根據此一選項，可省略操作302及303，且AF-1可基於中繼服務碼產生發現密鑰。

【0061】 在操作303，AF-2 (UE至網路中繼)產生用於發現UE至網路中繼之發現密鑰，且將其提供在傳輸至AF-1 (遠端UE)之密鑰回應訊息(亦被稱為一密鑰回應，如圖3A中展示)中。

【0062】 在操作304，AF-1 (遠端UE)將包含發現密鑰之用於發現之密鑰回應訊息(在圖3A中展示為用於發現之一密鑰回應)轉發至UE。

【0063】 在操作305，遠端UE藉由起始包含中繼服務碼之用於PC5通信之一密鑰請求訊息(展示為用於PC5通信之一密鑰請求)來聯繫AF-1 (遠端UE)。如本文中使用，用於通信之一密鑰請求訊息可包含用於PC5通信之密鑰請求訊息。

【0064】 在操作306，AF-1 (遠端UE)產生用於PC5通信之密鑰(展示為操作307之「密鑰」)且將其與一密鑰ID一起提供在傳輸至遠端UE之用於PC5通信之密鑰回應訊息(展示為圖3A之用於PC5通信之密鑰回應)中。如本文中使用，術語用於通信之密鑰(亦被稱為一通信密鑰)可被定義為包含用於PC5通信之密鑰、用於側鏈路通信之一密鑰等。因此，用於PC5通信之密鑰回應訊息包含用於PC5通信之密鑰及用於PC5通信之密鑰之密鑰識別符ID，且AF-1將用於PC5通信之密鑰回應訊息傳輸至遠端UE。如本文中使用，用於通信之一密鑰回應訊息可包含用於PC5通信之密鑰回應訊息。

【0065】 如上文關於操作300b論述，UE至網路中繼聯繫其本籍PLMN中之5G DNNMF以擷取定位於其本籍PLMN中之用於ProSe密鑰管理之AF-2 (UE至網路中繼)之位址。

【0066】 在操作307，UE至網路中繼藉由起始包含中繼服務碼之用於發現之一密鑰請求訊息(在圖3A中展示為用於發現之一密鑰請求)來聯繫

AF-2 (UE至網路中繼)，該中繼服務碼基於來自操作300b之AF-2之位址傳輸至AF-2。AF-2 (UE至網路中繼)從中繼服務碼自行產生發現密鑰。

【0067】 在操作308，AF-2 (UE至網路中繼)在傳輸至UE至網路中繼之用於發現之密鑰回應訊息(在圖3B中展示為用於發現之密鑰回應)中提供發現密鑰。

【0068】 在操作309，UE至網路中繼發現可使用模型A或模型B發現在PC5介面上發生。在使用模型A或模型B發現的情況下，遠端UE可基於從UE至網路中繼接收之一經加密發現訊息(例如，模型A之經加密發現通告訊息，或模型B之經加密發現回應訊息)來變得知道UE至網路中繼。更特定言之，UE至網路中繼可基於來自操作308之發現密鑰來加密/傳輸經加密發現訊息，遠端UE可使用來自操作304之發現密鑰來接收/解密經加密發現訊息，且操作304及308之發現密鑰可為相同的(此係因為其等係基於同一中繼服務碼)。

【0069】 在使用模型A發現的情況下，UE至網路中繼可廣播基於操作308之發現密鑰加密之一經加密發現通告訊息，且遠端UE使用操作304之發現密鑰接收/解密經加密發現通告訊息。

【0070】 在使用模型B發現的情況下，遠端UE傳輸基於操作304之發現密鑰加密之一經加密發現請求訊息，且UE至網路中繼可使用操作308之發現密鑰接收/解密經加密發現請求訊息。回應於接收/解密經加密發現請求訊息，UE至網路中繼可將(基於操作308之發現密鑰加密之)一經加密發現回應訊息傳輸至遠端UE，且遠端UE可使用操作304之發現密鑰接收/解密經加密發現回應訊息。

【0071】 在操作310，回應於在操作309發現UE至網路中繼，遠端

UE在PC5介面上將一直接通信請求(在圖3B中展示為直接通信請求(Direct comm req))發送至UE至網路中繼。遠端UE包含AF-1 (遠端UE)之位址及從AF-1 (遠端UE)接收之密鑰ID (即，來自操作306之用於PC5通信密鑰之密鑰ID)以及中繼服務碼。可在未經加密情況下傳輸/接收直接通信請求，或可使用操作304及308之發現密鑰加密/解密直接通信請求。

【0072】 當遠端UE發現其附近之一UE至網路中繼時，其在PC5介面上將AF-1 (遠端UE)之位址(例如，IP位址或FQDN)顯式地發送至UE至網路中繼。

【0073】 替代地，UE至網路中繼(亦被稱為一中繼UE)亦可使用遠端UE資訊以從其5G DDNMF查詢AF-2位址。

【0074】 存在關於UE至網路中繼可如何獲得PC5通信密鑰以支援遠端UE與網路之間的中繼通信之兩個選項/替代方案，且此等選項在下文關於選項1及選項2 (其等可為相互排斥之替代方案/選項)進行論述。

【0075】 下文關於圖3B之操作311、312、313及314論述選項1。

【0076】 在操作311，回應於接收到操作310之直接通信請求，UE至網路中繼聯繫AF-2 (UE至網路中繼)且在包含密鑰ID (來自操作310之直接通信請求)之用於PC5通信之密鑰請求訊息(在圖3B中展示為用於PC5通信之密鑰請求)中包含AF-1 (遠端UE)之位址。

【0077】 在操作312，AF-2 (UE至網路中繼)聯繫AF-1 (遠端UE)且轉發密鑰請求訊息(包含密鑰ID)。

【0078】 在操作313，回應於接收到操作312之密鑰請求，AF-1 (遠端UE)在傳輸至AF-2 (遠端UE)之密鑰回應訊息中包含由密鑰ID識別之用於PC5通信之密鑰。

【0079】 在操作314，AF-2 (UE至網路中繼)將包含密鑰之用於PC5通信之密鑰回應訊息(展示為用於PC5通信之密鑰回應)轉發至UE至網路中繼。

【0080】 下文關於圖3B之操作311a及311b論述選項2。

【0081】 在操作311a，回應於接收到操作310之直接通信請求，UE至網路中繼使用AF-1 (遠端UE)之位址，且藉由起始包含密鑰ID之用於PC5通信之密鑰請求訊息(展示為圖3B之用於PC5通信之密鑰請求)來直接聯繫AF-1 (遠端UE)。

【0082】 在操作311b，回應於接收到操作311a之用於PC5通信之密鑰請求訊息，AF-1 (遠端UE)在傳輸至UE至網路中繼之用於PC5通信之密鑰回應訊息(展示為用於PC5通信之密鑰回應)中包含由密鑰ID識別之用於PC5通信之密鑰。

【0083】 在完成選項1之操作311、312、313及314之後，或在完成選項2之操作311a及311b之後，UE至網路中繼及遠端UE兩者皆具有用於PC5通信之密鑰，該密鑰可用於加密/解密遠端UE與UE至網路中繼之間的PC5通信(亦被稱為中繼通信)。

【0084】 在操作315，UE至網路中繼在PC5上使用一直接通信回應來回應遠端。UE至網路中繼使用用於PC5通信之密鑰加密/傳輸直接通信回應，且遠端UE使用用於PC5通信之密鑰接收/解密直接通信回應。

【0085】 雖然圖3A至圖3B中未展示，但在於遠端UE處接收到直接通信回應訊息之後，遠端UE與通信網路之一無線電存取網路RAN節點之間的上行鏈路/下行鏈路通信可透過UE至網路中繼使用用於PC5通信之密鑰來加密/解密遠端UE與UE至網路中繼之間的通信而中繼。

【0086】 關於發現密鑰，亦可存在存在一個密鑰伺服器(或複數個密鑰伺服器)之一選項。例如，AF-1及AF-2兩者皆可向同一密鑰伺服器請求與一特定中繼服務碼相關聯之發現密鑰。當然，UE可直接聯繫伺服器，但若密鑰伺服器僅可由某些應用功能AF存取，則可存在更多安全性。可由ProSe商業服務之一第三方(並非一網路營運商)或某一主管機構維持(若干)密鑰伺服器。根據此等選項，當AF-1從遠端UE接收發現密鑰請求時，其聯繫密鑰伺服器以獲得發現密鑰。當AF-2從中繼UE接收發現密鑰請求時，其聯繫密鑰伺服器以獲得發現密鑰。若存在多個此等密鑰伺服器，則AF可使用中繼服務碼來判定聯繫哪一密鑰伺服器，例如使用一映射。

【0087】 現將參考根據發明概念之一些實施例之圖7之流程圖論述一遠端無線裝置(在圖3A至圖3B中展示為「遠端UE」，且使用圖4之方塊圖之通信裝置400結構實施)之操作。例如，模組可儲存於圖4之記憶體405中，且此等模組可提供指令，使得當由各自通信裝置處理電路403執行一模組之指令時，處理電路403執行流程圖之各自操作。

【0088】 在方塊700，處理電路403 (透過收發器401)獲得與遠端通信裝置相關聯之應用功能節點(AF-1)之一位址。可如上文關於圖3A之操作300a所論述般執行方塊700之操作。例如，可藉由從與遠端通信裝置相關聯之一直接發現名稱管理功能(DDNMF)節點提取與遠端通信裝置相關聯之應用功能節點(AF-1)之位址來獲得該位址。

【0089】 在方塊701，處理電路403 (透過收發器401)將用於發現之一密鑰請求訊息傳輸至與遠端通信裝置相關聯之一應用功能節點(AF-1)，其中密鑰請求訊息包含一中繼服務碼。可如上文關於圖3A之操作301所論述般執行方塊701之操作。例如，可基於在方塊700獲得之與遠端通信裝

置相關聯之應用功能節點(AF-1)之位址將用於發現之密鑰請求訊息傳輸至與遠端通信裝置相關聯之應用功能節點(AF-1)。

【0090】 在方塊704，處理電路403可(透過收發器401)接收一發現密鑰。可如上文關於圖3A之操作304所論述般執行方塊704之操作。例如，可藉由從與遠端通信裝置相關聯之應用功能節點(AF-1)接收包含發現密鑰之用於發現之一密鑰回應訊息來接收發現密鑰，其中用於發現之密鑰回應訊息與用於發現之密鑰請求訊息相關聯。

【0091】 在方塊705，處理電路403 (透過收發器401)將用於通信之一密鑰請求訊息傳輸至與遠端通信裝置相關聯之應用功能節點(AF-1)，其中用於通信之密鑰請求訊息包含中繼服務碼。可如上文關於圖3A之操作305所論述般執行方塊705之操作。例如，可基於與遠端通信裝置相關聯之應用功能節點(AF-1)之位址將用於通信之密鑰請求訊息傳輸至與遠端通信裝置相關聯之應用功能節點(AF-1)。

【0092】 在方塊706，處理電路403 (透過收發器401)接收一通信密鑰及用於通信密鑰之一密鑰識別符ID。可如上文關於圖3A之操作306所論述般執行方塊705之操作。例如，接收通信密鑰及用於通信密鑰之密鑰ID可包含接收包含通信密鑰及用於通信密鑰之密鑰ID之用於通信之一密鑰回應訊息，其中用於通信之密鑰回應訊息與用於通信之密鑰請求訊息相關聯。

【0093】 在方塊709，處理電路403發現一中繼通信裝置，其中發現中繼通信裝置包含：從中繼通信裝置接收一經加密發現訊息；及使用發現密鑰解密經加密發現訊息。可如上文關於圖3B之操作309所論述般執行方塊709之操作。例如，經加密發現訊息可包含由中繼通信裝置廣播且由處

理電路403 (透過收發器401)接收之一經加密發現通告訊息。在一替代方案中，發現中繼通信裝置可包含處理電路403 (透過收發器401)傳輸基於發現密鑰加密之一經加密發現請求訊息，其中經加密發現訊息係對應於經加密發現請求訊息之一經加密發現回應訊息，且其中經加密發現回應訊息由處理電路403 (透過收發器401)接收且使用發現密鑰解密。

【0094】 在方塊710，處理電路403回應於接收及解密來自中繼通信裝置之經加密發現訊息而(透過收發器401)將一直接通信請求傳輸至中繼通信裝置，其中直接通信請求包含用於通信密鑰之密鑰ID。可如上文關於圖3B之操作310所論述般執行方塊701之操作。例如，傳輸直接通信請求可包含使用發現密鑰加密直接通信請求以提供一經加密直接通信請求，且(透過收發器401)傳輸經加密直接通信請求。另外，直接通信請求可包含與遠端通信裝置相關聯之應用功能節點(AF-1)之位址，及/或直接通信請求可包含中繼服務碼。

【0095】 在方塊715，處理電路403 (透過收發器401)從中繼通信裝置接收一經加密直接通信回應，其中接收經加密直接通信回應包含解密經加密直接通信回應。可如上文關於圖3B之操作315所論述般執行方塊715之操作。

【0096】 在方塊717，處理電路403 (透過收發器401)提供使用通信密鑰提供與一無線電存取網路RAN節點之通信，其中與RAN節點之通信透過中繼通信裝置中繼。例如，提供通信可包含使用通信密鑰加密通信以提供一經加密通信，且(透過收發器401)將經加密通信傳輸至中繼通信裝置，及/或提供通信可包含(透過收發器401)從中繼通信裝置接收一經加密通信，且使用通信密鑰解密經加密通信以提供來自RAN節點之通信。

【0097】 關於通信裝置及相關方法之一些實施例，來自圖7之流程圖之各種操作可為選用的。例如，關於實例實施例1 (下文闡述)之方法，圖7之方塊700、701、705及/或717之操作可為選用的。

【0098】 現將參考根據發明概念之一些實施例之圖8之流程圖論述一中繼通信裝置(在圖3A至圖3B中展示為「UE至NW中繼」，且使用圖4之方塊圖之通信裝置400結構實施)之操作。例如，模組可儲存於圖4之記憶體405中，且此等模組可提供指令，使得當由各自通信裝置處理電路403執行一模組之指令時，處理電路403執行流程圖之各自操作。

【0099】 在方塊800，處理電路403 (透過收發器401)獲得與中繼通信裝置相關聯之應用功能節點(AF-2)之一位址。可如上文關於圖3A之操作300b所論述般執行方塊800之操作。例如，獲得位址可包含從與中繼通信裝置相關聯之一直接發現名稱管理功能DDNMF節點提取與中繼通信裝置相關聯之應用功能節點(AF-2)之位址。

【0100】 在方塊807，處理電路403 (透過收發器401)將用於發現之一密鑰請求訊息傳輸至與中繼通信裝置相關聯之一應用功能節點(AF-2)，其中密鑰請求訊息包含一中繼服務碼。可如上文關於圖3A之操作307所論述般執行方塊807之操作。例如，可基於與中繼通信裝置相關聯之應用功能節點(AF-2)之位址將用於發現之密鑰請求訊息傳輸至與中繼通信裝置相關聯之應用功能節點(AF-2)。

【0101】 在方塊808，處理電路403 (透過收發器401)接收一發現密鑰。可如上文關於圖3B之操作308所論述般執行方塊808之操作。例如，接收發現密鑰可包含從與中繼通信裝置相關聯之應用功能節點(AF-2)接收包含發現密鑰之用於發現之一密鑰回應訊息，其中用於發現之密鑰回應訊

息與用於發現之密鑰請求訊息相關聯。

【0102】 在方塊809，處理電路403 (透過收發器401)傳輸一經加密發現訊息，其中使用發現密鑰加密經加密發現訊息。可如上文關於圖3B之操作309所論述般執行方塊809之操作。例如，經加密發現訊息可為由中繼通信裝置(藉由處理電路403透過收發器401)廣播之一經加密發現通告訊息。在一替代方案中，處理電路403可(透過收發器401)接收一經加密發現請求訊息，其中接收經加密發現請求訊息包含使用發現密鑰解密經加密發現請求訊息；且經加密發現訊息可為回應於經加密發現請求訊息而(藉由處理電路403透過收發器401)傳輸之一經加密發現回應訊息，其中使用發現密鑰加密經加密發現回應訊息。

【0103】 在方塊810，處理電路403 (透過收發器401)從一遠端通信裝置接收一直接通信請求，其中直接通信請求包含一密鑰ID。可如上文關於圖3B之操作310所論述般執行方塊810之操作。例如，接收直接通信請求可包含處理電路403 (透過收發器401)接收一經加密直接通信請求，且使用發現密鑰解密經加密直接通信請求以提供直接通信請求。再者，直接通信請求可包含中繼服務代碼，及/或直接通信請求可包含與遠端通信裝置相關聯之一應用功能節點(AF-1)之一位址。

【0104】 在方塊811，處理電路403可(透過收發器401)獲得對應於來自直接通信請求之密鑰ID之一通信密鑰。可在上文關於圖3B之操作311及314或關於圖3B之操作311a及311b所論述般執行方塊811之操作。在對應於圖3B之操作311及314之一替代方案(展示為選項1)中，處理電路403可回應於接收到直接通信訊息而(透過收發器401)將用於通信之一密鑰請求訊息傳輸至與中繼通信裝置相關聯之應用功能節點(AF-2)，其中用於通

信之密鑰請求訊息包含密鑰ID及與遠端通信裝置相關聯之應用功能節點(AF-1)之位址；且處理電路403可(透過收發器401)從與中繼通信裝置相關聯之應用功能節點(AF-2)接收用於通信之一密鑰回應訊息，其中密鑰回應訊息包含對應於密鑰ID之通信密鑰。在對應於圖3B之操作311a及311b之一替代方案(展示為選項2)中，處理電路403可回應於接收到直接通信訊息而(透過收發器401)使用與遠端通信裝置相關聯之應用功能節點(AF-1)之位址將用於通信之一密鑰請求訊息傳輸至與遠端通信裝置相關聯之應用功能節點(AF-1)，其中用於通信之密鑰請求訊息包含密鑰ID；且處理電路403可(透過收發器401)從與遠端通信裝置相關聯之應用功能節點(AF-1)接收用於通信之一密鑰回應訊息，其中密鑰回應訊息包含對應於密鑰ID之通信密鑰。

【0105】 在方塊815，處理電路403 (透過收發器401)將一經加密直接通信回應傳輸至遠端通信裝置，其中使用對應於密鑰ID之通信密鑰加密經加密直接通信回應。可如上文關於圖3B之操作315所論述般執行方塊815之操作。

【0106】 在方塊817，處理電路403 (透過收發器401)使用用於在遠端通信裝置與中繼通信裝置之間加密之通信密鑰中繼遠端通信裝置與一無線電存取網路RAN節點之間的通信。例如，中繼通信可包含從遠端通信裝置接收作為一經加密通信之通信，使用通信密鑰解密經加密通信，及將通信傳輸至RAN節點；及/或中繼通信可包含從RAN節點接收通信，使用通信密鑰加密通信以提供一經加密通信，及將經加密通信傳輸至遠端通信裝置。

【0107】 關於通信裝置及相關方法之一些實施例，來自圖8之流程

圖之各種操作可為選用的。例如，關於實例實施例13 (下文闡述)之方法，圖8之方塊800、807及/或817之操作可為選用的。

【0108】 現將參考根據發明概念之一些實施例之圖9之流程圖論述一應用功能節點(在圖3A至圖3B中展示為「AF-1 (遠端UE)」，且使用圖6之方塊圖之核心網路CN節點600結構實施)之操作。例如，模組可儲存於圖6之記憶體605中，且此等模組可提供指令，使得當由各自CN節點處理電路603執行一模組之指令時，處理電路603執行流程圖之各自操作。

【0109】 在方塊901，處理電路603 (透過網路介面607)從遠端通信裝置接收用於發現之一密鑰請求訊息，其中密鑰請求訊息包含一中繼服務碼。可如上文關於圖3A之操作301所論述般執行方塊901之操作。

【0110】 在方塊902，處理電路603基於包含於用於發現之密鑰請求訊息中之中繼服務碼獲得一發現密鑰。例如，處理電路603可藉由基於中繼服務碼在內部導出發現密鑰來獲得發現密鑰。在一替代方案中，處理電路603可藉由以下步驟獲得發現密鑰：回應於接收到用於發現之密鑰請求訊息而(透過網路介面607)將一密鑰請求訊息傳輸(操作302)至與一中繼通信裝置相關聯之一應用功能節點(AF-2)，其中密鑰請求訊息包含中繼服務碼(例如，如上文關於圖3A之操作302論述)；及(透過網路介面607)從與中繼通信裝置相關聯之應用功能節點(AF-2)接收(操作303)一密鑰回應訊息，其中密鑰回應訊息包含發現密鑰(例如，如上文關於圖3A之操作303論述)。在對應於圖3A之操作302及303之替代方案中，傳輸圖3A之操作302之密鑰請求訊息可包含轉發圖3A之操作301之用於發現之密鑰請求訊息。

【0111】 在方塊904，處理電路603 (透過網路介面607)將包含發現

密鑰之用於發現之一密鑰回應訊息傳輸至遠端通信裝置。可如上文關於圖3A之操作304所論述般執行方塊904之操作。在對應於圖3A之操作302及303之替代方案中，傳輸操作304之用於發現之密鑰回應訊息可包含轉發圖3A之操作303之密鑰回應訊息。

【0112】 在方塊905a，處理電路603 (透過網路介面607)從遠端通信裝置接收用於通信之一密鑰請求訊息，其中用於通信之密鑰請求訊息包含中繼服務碼。可如上文關於圖3A之操作305所論述般執行方塊905之操作。

【0113】 在方塊905b，處理電路603基於中繼服務碼獲得一通信密鑰及用於通信密鑰之一密鑰ID。

【0114】 在方塊906，處理電路603將用於通信之一密鑰回應訊息傳輸至遠端通信裝置，其中密鑰回應訊息包含通信密鑰及用於通信密鑰之密鑰ID。可如上文關於圖3A之操作306所論述般執行方塊906之操作。

【0115】 在方塊912，處理電路603 (透過網路介面607)接收包含密鑰ID之一密鑰請求訊息。

【0116】 在方塊913，處理電路603回應於接收到包含密鑰ID之密鑰請求訊息而(透過網路介面607)傳輸包含通信密鑰之一密鑰回應訊息。

【0117】 例如，可如上文關於圖3B之操作312及313所論述般執行方塊912及913之操作(展示為選項1)。在此等實施例中：在方塊912，處理電路603 (透過網路介面607)從與一中繼通信裝置相關聯之一應用功能節點(AF-2)接收包含密鑰ID之密鑰請求訊息(如上文關於圖3B之操作312論述)；且在方塊913，處理電路603回應於接收到包含密鑰ID之密鑰請求訊息而(透過網路介面607)將包含通信密鑰之密鑰回應訊息傳輸至與一中繼

通信裝置相關聯之應用功能節點(AF-2) (如上文關於圖3B之操作313論述)。

【0118】 在額外或替代實施例中，可如上文關於圖3B之操作311a及311b所論述般執行方塊912及913之操作(展示為選項2)。在此等實施例中：在方塊912，處理電路603 (透過網路介面607)從一中繼通信裝置接收包含密鑰ID之密鑰請求訊息(如上文關於圖3B之操作311a論述)；且在方塊913，處理電路603回應於接收到包含密鑰ID之密鑰請求訊息而(透過網路介面607)將包含通信密鑰之密鑰回應訊息傳輸至中繼通信裝置(如上文關於圖3B之操作311b論述)。

【0119】 關於CN節點及相關方法之一些實施例，來自圖9之流程圖之各種操作可為選用的。例如，關於實例實施例27 (下文闡述)之方法，圖9之方塊905a、905b、906、912及/或913之操作可為選用的。

【0120】 現將參考根據發明概念之一些實施例之圖10之流程圖論述一應用功能節點(在圖3A至圖3B中展示為「AF-2 (UE至網路中繼)」，且使用圖6之方塊圖之核心網路CN節點600結構實施)之操作。例如，模組可儲存於圖6之記憶體605中，且此等模組可提供指令，使得當由各自CN節點處理電路603執行一模組之指令時，處理電路603執行流程圖之各自操作。

【0121】 在方塊1002a，處理電路603 (透過網路介面607)從與遠端通信裝置相關聯之一應用功能節點(AF-1)接收一密鑰請求訊息，其中密鑰請求訊息包含一中繼服務碼。可如上文關於圖3A之操作302所論述般執行方塊1002a之操作。

【0122】 在方塊1002b，處理電路603基於包含於來自與遠端通信裝

置相關聯之應用功能節點(AF-1)之密鑰請求訊息中之中繼服務碼獲得一發現密鑰。

【0123】 在方塊1003，處理電路603 (透過網路介面607)將包含(在方塊1002b獲得之)發現密鑰之一密鑰回應訊息傳輸至與遠端通信裝置相關聯之應用功能節點(AF-1)。可如上文關於圖3A之操作303所論述般執行方塊1003之操作。

【0124】 在方塊1007a，處理電路603 (透過網路介面607)從中繼通信裝置接收用於發現之一密鑰請求訊息，其中密鑰請求訊息包含中繼服務碼。可如上文關於圖3A之操作307所論述般執行方塊1007之操作。

【0125】 在方塊1007b，處理電路603基於包含於用於發現之密鑰請求訊息中之中繼服務碼獲得一發現密鑰。

【0126】 在方塊1008，處理電路(透過網路介面607)將包含發現密鑰之用於發現之一密鑰回應訊息傳輸至中繼通信裝置。可如上文關於圖3B之操作308所論述般執行方塊1008之操作。例如，處理電路603可藉由基於中繼服務碼在內部導出發現密鑰來獲得發現密鑰。

【0127】 在方塊1011，處理電路603 (透過網路介面607)從中繼通信裝置接收用於通信之一密鑰請求訊息，其中用於通信之密鑰請求訊息包含一密鑰ID。可如上文關於圖3B之操作311所論述般執行方塊1011之操作。

【0128】 在方塊1012，處理電路603 (透過網路介面607)將包含密鑰ID之一密鑰請求訊息傳輸至與一遠端通信裝置相關聯之一應用功能(AF-1)。可如上文關於圖3B之操作312所論述般執行方塊1012之操作。例如，傳輸密鑰請求訊息可包含轉發(在方塊1011接收之)用於通信之密鑰請求訊息。

【0129】 在方塊1013，處理電路603 (透過網路介面607)接收包含對應於密鑰ID之一通信密鑰之一密鑰回應訊息(來自AF-1)，其中密鑰回應訊息對應於密鑰請求訊息。可如上文關於圖3B之操作313所論述般執行方塊1013之操作。

【0130】 在方塊1014，處理電路603回應於接收到密鑰回應訊息而(透過網路介面607)將包含通信密鑰之用於通信之一密鑰回應訊息傳輸至中繼通信節點。可如上文關於圖3B之操作314所論述般執行方塊1014之操作。例如，傳輸用於通信之密鑰回應訊息可包含轉發(在方塊1013接收之)密鑰回應訊息。

【0131】 關於CN節點及相關方法之一些實施例，來自圖10之流程圖之各種操作可為選用的。例如，關於實例實施例33 (下文闡述)之方法，圖10之方塊1007a、1007b、1008、1011、1012、1013及/或1014之操作可為選用的。

【0132】 下文論述實例實施例。

【0133】 實施例1.一種操作一遠端通信裝置之方法，該方法包括：

接收(704)一發現密鑰；

接收(706)一通信密鑰及用於該通信密鑰之一密鑰識別符ID；

發現(709)一中繼通信裝置，其中發現該中繼通信裝置包含從該中繼通信裝置接收一經加密發現訊息，且使用該發現密鑰解密該經加密發現訊息；

回應於接收及解密來自該中繼通信裝置之該經加密發現訊息而將一直接通信請求傳輸(710)至該中繼通信裝置，其中該直接通信請求包含用於該通信密鑰之該密鑰ID；及

從該中繼通信裝置接收(715)一經加密直接通信回應，其中接收該經加密直接通信回應包含解密該經加密直接通信回應。

2.如實施例1之方法，其中傳輸該直接通信請求包括使用該發現密鑰加密該直接通信請求以提供一經加密直接通信請求，且傳輸該經加密直接通信請求。

3.如實施例1至2中任一項之方法，其進一步包括：

將用於發現之一密鑰請求訊息傳輸(701)至與該遠端通信裝置相關聯之一應用功能節點(AF-1)，其中該密鑰請求訊息包含一中繼服務碼；及

將用於通信之一密鑰請求訊息傳輸(705)至與該遠端通信裝置相關聯之該應用功能節點(AF-1)，其中用於通信之該密鑰請求訊息包含該中繼服務碼；

其中接收該發現密鑰包括從與該遠端通信裝置相關聯之該應用功能節點(AF-1)接收包含該發現密鑰之用於發現之一密鑰回應訊息，且其中用於發現之該密鑰回應訊息與用於發現之該密鑰請求訊息相關聯；

其中接收該通信密鑰及用於該通信密鑰之該密鑰ID包括接收包含該通信密鑰及用於該通信密鑰之該密鑰ID之用於通信之一密鑰回應訊息，且其中用於通信之該密鑰回應訊息與用於通信之該密鑰請求訊息相關聯。

4.如實施例3之方法，其進一步包括：

獲得(700)與該遠端通信裝置相關聯之該應用功能節點(AF-1)之一位址；

其中基於與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於發現之該密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)；

其中基於與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於通信之該密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)。

5.如實施例4之方法，其中獲得該位址包括從與該遠端通信裝置相關聯之一直接發現名稱管理功能DDNMF節點提取與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址。

6.如實施例4至5中任一項之方法，其中該直接通信請求包含與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址。

7.如實施例3至6中任一項之方法，其中該直接通信請求包含該中繼服務碼。

8.如實施例1至7中任一項之方法，其中該經加密發現訊息包括由該中繼通信裝置廣播之一經加密發現通告訊息。

9.如實施例1至7中任一項之方法，其中發現該中繼通信裝置包括傳輸基於該發現密鑰加密之一經加密發現請求訊息，且其中該經加密發現訊息包括對應於該經加密發現請求訊息之一經加密發現回應訊息，且其中使用該發現密鑰解密該經加密發現回應訊息。

10.如實施例1至9中任一項之方法，其進一步包括：

使用該通信密鑰提供(717)與一無線電存取網路RAN節點之通信，其中與該RAN節點之該通信係透過該中繼通信裝置中繼。

11.如實施例10之方法，其中提供該通信包括使用該發現密鑰加密該通信以提供一經加密通信，且將該經加密通信傳輸至該中繼通信裝置。

12.如實施例10之方法，其中提供該通信包括從該中繼通信裝置接收一經加密通信，且使用該通信密鑰解密該經加密通信以提供來自該RAN

節點之該通信。

13.一種操作一中繼通信裝置之方法，該方法包括：

接收(808)一發現密鑰；

傳輸(809)一經加密發現訊息，其中使用該發現密鑰加密該經加密發現訊息；

從一遠端通信裝置接收(810)一直接通信請求，其中該直接通信請求包含一密鑰ID；

獲得(811)對應於來自該直接通信請求之該密鑰ID之一通信密鑰；及

將一經加密直接通信回應傳輸(815)至該遠端通信裝置，其中使用對應於該密鑰ID之該通信密鑰加密該經加密直接通信回應。

14.如實施例13之方法，其中接收該直接通信請求包括接收一經加密直接通信請求，且使用該發現密鑰解密該經加密直接通信請求以提供該直接通信請求。

15.如實施例13至14中任一項之方法，其進一步包括：

將用於發現之一密鑰請求訊息傳輸(807)至與該中繼通信裝置相關聯之一應用功能節點(AF-2)，其中該密鑰請求訊息包含一中繼服務碼；及

其中接收該發現密鑰包括從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收包含該發現密鑰之用於發現之一密鑰回應訊息，且其中用於發現之該密鑰回應訊息與用於發現之該密鑰請求訊息相關聯。

16.如實施例15之方法，其進一步包括：

獲得(800)與該中繼通信裝置相關聯之該應用功能節點(AF-2)之一位址；

其中基於與該中繼通信裝置相關聯之該應用功能節點(AF-2)之該位

址將用於發現之該密鑰請求訊息傳輸至與該中繼通信裝置相關聯之該應用功能節點(AF-2)。

17.如實施例16之方法，其中獲得該位址包括從與該中繼通信裝置相關聯之一直接發現名稱管理功能DDNMF節點提取與該中繼通信裝置相關聯之該應用功能節點(AF-2)之該位址。

18.如實施例15至17中任一項之方法，其中該直接通信請求包含該中繼服務碼。

19.如實施例15至18中任一項之方法，其中該直接通信請求包含與該遠端通信裝置相關聯之一應用功能節點(AF-1)之一位址。

20.如實施例19之方法，其中獲得該通信密鑰包括，

回應於接收到該直接通信訊息而將用於通信之一密鑰請求訊息傳輸至與該中繼通信裝置相關聯之該應用功能節點(AF-2)，其中用於通信之該密鑰請求訊息包含該密鑰ID及與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址，及

從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收用於通信之一密鑰回應訊息，其中該密鑰回應訊息包含對應於該密鑰ID之該通信密鑰。

21.如實施例19之方法，其中獲得該通信密鑰包括，

回應於接收到該直接通信訊息而使用與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於通信之一密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)，其中用於通信之該密鑰請求訊息包含該密鑰ID，及

從與該遠端通信裝置相關聯之該應用功能節點(AF-1)接收用於通信

之一密鑰回應訊息，其中該密鑰回應訊息包含對應於該密鑰ID之該通信密鑰。

22.如實施例13至21中任一項之方法，其中該經加密發現訊息包括由該中繼通信裝置廣播之一經加密發現通告訊息。

23.如實施例13至21中任一項之方法，其進一步包括：

接收一經加密發現請求訊息，其中接收該經加密發現請求訊息包含使用發現密鑰解密該經加密發現請求訊息，及

其中該經加密發現訊息包括回應於該經加密發現請求訊息而傳輸之一經加密發現回應訊息，且其中使用該發現密鑰加密該經加密發現回應訊息。

24.如實施例13至23中任一項之方法，其進一步包括：

使用用於在該遠端通信裝置與該中繼通信裝置之間加密之該通信密鑰中繼(817)該遠端通信裝置與一無線電存取網路RAN節點之間的通信。

25.如實施例24之方法，其中中繼該通信包括從該遠端通信裝置接收作為一經加密通信之該通信，使用該通信密鑰解密該經加密通信，且將該通信傳輸至該RAN節點。

26.如實施例24之方法，其中中繼該通信包括從該RAN節點接收該通信，使用該通信密鑰加密該通信以提供一經加密通信，且將該經加密通信傳輸至該遠端通信裝置。

27.一種操作與一遠端通信裝置相關聯之一應用功能節點(AF-1)之方法，該方法包括：

從該遠端通信裝置接收(901)用於發現之一密鑰請求訊息，其中該密鑰請求訊息包含一中繼服務碼；

基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得(902)一發現密鑰；及

將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸(904)至該遠端通信裝置。

28.如實施例27之方法，其中獲得該發現密鑰包括基於該中繼服務碼在內部導出該發現密鑰。

29.如實施例27之方法，其中獲得(902)該發現密鑰包括，

回應於接收到用於發現之該密鑰請求訊息而將一密鑰請求訊息傳輸至與一中繼通信裝置相關聯之一應用功能節點(AF-2)，其中該密鑰請求訊息包含該中繼服務碼，及

從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收一密鑰回應訊息，其中該密鑰回應訊息包含該發現密鑰。

30.如實施例29之方法，其中傳輸該密鑰請求訊息包括轉發用於發現之該密鑰請求訊息，且其中傳輸用於發現之該密鑰回應訊息包括轉發該密鑰回應訊息。

31.如實施例27至30中任一項之方法，其進一步包括：

從該遠端通信裝置接收(905a)用於通信之一密鑰請求訊息，其中用於通信之該密鑰請求訊息包含該中繼服務碼；

基於該中繼服務碼獲得(905b)一通信密鑰及用於該通信密鑰之一密鑰ID；及

將用於通信之一密鑰回應訊息傳輸(906)至該遠端通信裝置，其中該密鑰回應訊息包含該通信密鑰及用於該通信密鑰之該密鑰ID。

32.如實施例31之方法，其進一步包括：

接收(912)一密鑰請求訊息，其中該密鑰請求訊息包含該密鑰ID；及

回應於接收到包含該密鑰ID之該密鑰請求訊息而傳輸(913)包含該通信密鑰之一密鑰回應訊息。

33.一種操作與一中繼通信裝置相關聯之一應用功能節點(AF-2)之方法，該方法包括：

從該中繼通信裝置接收(1007a)用於發現之一密鑰請求訊息，其中該密鑰請求訊息包含一中繼服務碼；

基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得(1007b)一發現密鑰；及

將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸(1008)至該中繼通信裝置。

34.如實施例33之方法，其中獲得該發現密鑰包括基於該中繼服務碼在內部導出該發現密鑰。

35.如實施例33至34中任一項之方法，其進一步包括：

從該中繼通信裝置接收(1011)用於通信之一密鑰請求訊息，其中用於通信之該密鑰請求訊息包含一密鑰ID；

將包含該密鑰ID之一密鑰請求訊息傳輸(1012)至與一遠端通信裝置相關聯之一應用功能(AF-1)；

接收(1013)包含對應於該密鑰ID之一通信密鑰之一密鑰回應訊息，其中該密鑰回應訊息對應於該密鑰請求訊息；及

回應於接收到該密鑰回應訊息而將包含該通信密鑰之用於通信之一密鑰回應訊息傳輸(1014)至該中繼通信節點。

36.如實施例35之方法，其中傳輸該密鑰請求訊息包括轉發用於通信

之該密鑰請求訊息，且其中傳輸用於通信之該密鑰回應訊息包括轉發該密鑰回應訊息。

37.如實施例35至36中任一項之方法，其進一步包括：

從與該遠端通信裝置相關聯之一應用功能節點(AF-1)接收(1002a)一密鑰請求訊息，其中該密鑰請求訊息包含該中繼服務碼；

基於包含於來自與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該密鑰請求訊息中之該中繼服務碼獲得(1002b)該發現密鑰；及

將包含該發現密鑰之一密鑰回應訊息傳輸(1003)至與該遠端通信裝置相關聯之該應用功能節點(AF-1)。

38.一種遠端通信裝置(400)，其包括：

處理電路(403)；及

記憶體(405)，其與該處理電路耦合，其中該記憶體包含當由該處理電路執行時導致該遠端通信裝置執行如實施例1至12中任一項之操作之指令。

39.一種遠端通信裝置(400)，其經調適以根據實施例1至12中任一項執行。

40.一種電腦程式，其包括待由一遠端通信裝置(400)之處理電路(403)執行之程式碼，藉此該程式碼之執行導致該遠端通信裝置(400)執行如實施例1至12中任一項之操作。

41.一種電腦程式產品，其包括一非暫時性儲存媒體，該非暫時性儲存媒體包含待由一遠端通信裝置(400)之處理電路(403)執行之程式碼，藉此該程式碼之執行導致該遠端通信裝置(400)執行如實施例1至12中任一項之操作。

42.一種中繼通信裝置(400)，其包括：

處理電路(403)；及

記憶體(405)，其與該處理電路耦合，其中該記憶體包含當由該處理電路執行時導致該中繼通信裝置執行如實施例13至26中任一項之操作之指令。

43.一種中繼通信裝置(400)，其經調適以根據實施例13至26中任一項執行。

44.一種電腦程式，其包括待由一中繼通信裝置(400)之處理電路(403)執行之程式碼，藉此該程式碼之執行導致該中繼通信裝置(400)執行如實施例13至26中任一項之操作。

45.一種電腦程式產品，其包括一非暫時性儲存媒體，該非暫時性儲存媒體包含待由一中繼通信裝置(400)之處理電路(403)執行之程式碼，藉此該程式碼之執行導致該中繼通信裝置(400)執行如實施例13至26中任一項之操作。

46.一種應用功能AF節點(600、AF-1)，其包括：

處理電路(603)；及

記憶體(605)，其與該處理電路耦合，其中該記憶體包含當由該處理電路執行時導致該AF節點執行如實施例27至32中任一項之操作之指令。

47.一種應用功能AF節點(600、AF-1)，其經調適以根據實施例27至32中任一項執行。

48.一種電腦程式，其包括待由一應用功能AF節點(600、AF-1)之處理電路(403)執行之程式碼，藉此該程式碼之執行導致該AF節點(600、AF-1)執行如實施例27至32中任一項之操作。

49.一種電腦程式產品，其包括一非暫時性儲存媒體，該非暫時性儲存媒體包含待由一應用功能AF節點(600、AF-1)之處理電路(603)執行之程式碼，藉此該程式碼之執行導致該AF節點(600、AF-1)執行如實施例27至32中任一項之操作。

50.一種應用功能AF節點(600、AF-2)，其包括：

處理電路(603)；及

記憶體(605)，其與該處理電路耦合，其中該記憶體包含當由該處理電路執行時導致該AF節點執行如實施例33至37中任一項之操作之指令。

51.一種應用功能AF節點(600、AF-2)，其經調適以根據實施例33至37中任一項執行。

52.一種電腦程式，其包括待由一應用功能AF節點(600、AF-2)之處理電路(603)執行之程式碼，藉此該程式碼之執行導致該AF節點(600、AF-2)執行如實施例33至37中任一項之操作。

53.一種電腦程式產品，其包括一非暫時性儲存媒體，該非暫時性儲存媒體包含待由一應用功能AF節點(600、AF-2)之處理電路(603)執行之程式碼，藉此該程式碼之執行導致該AF節點(600、AF-2)執行如實施例33至37中任一項之操作。

【0134】 下文論述進一步定義及實施例。

【0135】 在本發明概念之各種實施例之上文描述中，應理解，本文中使用之術語僅用於描述特定實施例之目的且不旨在限制本發明概念。除非另外定義，否則本文中使用之所有術語(包含技術及科學術語)具有與本發明概念所屬之技術之一般技術者普遍理解的相同之含義。將進一步理解，術語(諸如在常用字典中定義之術語)應被解釋為具有與其等在此說明

書及相關技術之內容脈絡中之含義一致之一含義且將不以一理想化或過度形式意義解釋，除非本文中明確如此定義。

【0136】 當一元件被稱為「連接」、「耦合」、「回應」或其等之變體於另一元件時，其可直接連接、耦合或回應於另一元件或可存在中介元件。相比之下，當一元件被稱為「直接連接」、「直接耦合」、「直接回應」或其等之變體於另一元件時，不存在中介元件。貫穿全文，相同數字指代相同元件。此外，如本文中使用之「耦合」、「連接」、「回應」或其等之變體可包含無線耦合、連接或回應。如本文中使用，單數形式「一」、「一個」及「該」亦旨在包含複數形式，除非內容脈絡另外明確指示。為簡潔及/或簡明起見，可不詳細描述熟知功能或構造。術語「及/或(縮寫為「/」)」包含相關聯列出品項之一或多者之任何者及全部組合。

【0137】 將理解，儘管術語第一、第二、第三等可在本文中用於描述各種元件/操作，然此等元件/操作不應受此等術語限制。此等術語僅用於區分一個元件/操作與另一元件/操作。因此，在不脫離本發明概念之教示的情況下，一些實施例中之一第一元件/操作可在其他實施例中被稱為一第二元件/操作。貫穿說明書，相同參考數字或相同參考指定符指示相同或類似元件。

【0138】 如本文中使用，術語「包括(comprise、comprising、comprises)」、「包含(include、including、includes)」、「具有(have、has、having)」或其等之變體係開放式的且包含一或多個所陳述特徵、整數、元件、步驟、組件或功能但不排除一或多個其他特徵、整數、元件、步驟、組件、功能或其等之群組之存在或添加。此外，如本文中使用，源於拉丁文片語「exempli gratia」之常見縮寫「e.g.(例如)」可用於介紹或

指定一先前提及品項之一或多個一般實例且不旨在限制此品項。源於拉丁文片語「id est」之常見縮寫「i.e.(即)」可用於指定來自一更一般引述之一特定品項。

【0139】 本文中參考電腦實施方法、設備(系統及/或裝置)及/或電腦程式產品之方塊圖及/或流程圖描述實例實施例。應理解，可藉由由一或多個電腦電路執行之電腦程式指令實施方塊圖及/或流程圖繪示之一方塊及方塊圖及/或流程圖繪示中之方塊組合。可將此等電腦程式指令提供至一通用電腦電路、專用電腦電路及/或其他可程式化資料處理電路之一處理器電路以產生一機器，使得經由電腦及/或其他可程式化資料處理裝置之處理器執行之指令變換及控制電晶體、儲存於記憶體位置中之值及此電路內之其他硬體組件以實施方塊圖及/或一或多個流程圖方塊中指定之功能/動作，且藉此產生用於實施方塊圖及/或(若干)流程圖方塊中指定之功能/動作之構件(功能性)及/或結構。

【0140】 此等電腦程式指令亦可儲存於一有形電腦可讀媒體中，該等電腦程式指令可引導一電腦或其他可程式化資料處理設備以一特定方式運作，使得儲存於電腦可讀媒體中之指令產生一製品，該製品包含實施方塊圖及/或一或多個流程圖方塊中指定之功能/動作之指令。因此，本發明概念之實施例可體現為硬體及/或在一處理器(諸如一數位信號處理器)上運行之軟體(包含韌體、常駐軟體、微碼等)，其等可被統稱為「電路」、「一模組」或其等之變體。

【0141】 亦應注意，在一些替代實施方案中，在方塊中提及之功能/動作可不按流程圖中提及之順序發生。例如，取決於所涉及之功能性/動作，連續展示之兩個方塊事實上可實質上同時執行，或方塊有時可按相反

順序執行。再者，流程圖及/或方塊圖之一給定方塊之功能性可被劃分為多個方塊，及/或流程圖及/或方塊圖之兩個或兩個以上方塊之功能性可至少部分整合。最後，在不脫離發明概念之範疇的情況下，可在所繪示之方塊之間添加/插入其他方塊，及/或可省略方塊/操作。再者，儘管一些圖包含通信路徑上之箭頭以展示一主要通信方向，然應理解，通信可在與所描繪箭頭相反之方向上發生。

【0142】 在實質上不脫離本發明概念之原理的情況下，可對實施例做出許多變化及修改。全部此等變化及修改旨在在本文中包含於本發明概念之範疇內。因此，上文揭示之標的物應被視為闡釋性且非限制性，且實施例之實例旨在涵蓋落入本發明概念之精神及範疇內之全部此等修改、增強及其他實施例。因此，在法律允許之最大範圍內，本發明概念之範疇應由包含實施例之實例及其等之等效物之本發明之最廣泛可容許解釋來判定，且不應被前述詳細描述限制(restricted或limited)。

【符號說明】

【0143】

300a: 操作

300b: 操作

301: 操作

302: 操作

303: 操作

304: 操作

305: 操作

306: 操作

307: 操作

308: 操作

309: 操作

310: 操作

311: 操作

311a: 操作

311b: 操作

312: 操作

313: 操作

314: 操作

315: 操作

400: 通信裝置UE/實體/遠端通信裝置

401: 收發器電路/收發器

403: 處理電路

405: 記憶體電路/記憶體

500: 無線電存取網路RAN節點

501: 收發器電路/收發器

503: 處理電路

505: 記憶體電路/記憶體

507: 網路介面電路/網路介面

600: 核心網路(CN)節點/實體

603: 處理電路

605: 記憶體電路/記憶體

607: 網路介面電路/網路介面

700: 方塊

701: 方塊

704: 方塊

705: 方塊

706: 方塊

709: 方塊

710: 方塊

715: 方塊

717: 方塊

800: 方塊

807: 方塊

808: 方塊

809: 方塊

810: 方塊

811: 方塊

815: 方塊

817: 方塊

901: 方塊

902: 方塊

904: 方塊

905a: 方塊

905b: 方塊

906: 方塊

912: 方塊

913: 方塊

1002a: 方塊

1002b: 方塊

1003: 方塊

1007a: 方塊

1007b: 方塊

1008: 方塊

1011: 方塊

1012: 方塊

1013: 方塊

1014: 方塊

【發明申請專利範圍】

【請求項1】

一種操作一遠端通信裝置之方法，該方法包括：

接收(704)一發現密鑰；

接收(706)一通信密鑰及用於該通信密鑰之一密鑰識別符ID；

發現(709)一中繼通信裝置，其中發現該中繼通信裝置包含從該中繼通信裝置接收一經加密發現訊息，且使用該發現密鑰解密該經加密發現訊息；

回應於接收及解密來自該中繼通信裝置之該經加密發現訊息而將一直接通信請求傳輸(710)至該中繼通信裝置，其中該直接通信請求包含用於該通信密鑰之該密鑰ID；及

從該中繼通信裝置接收(715)一經加密直接通信回應，其中接收該經加密直接通信回應包含解密該經加密直接通信回應。

【請求項2】

如請求項1之方法，其中傳輸該直接通信請求包括：

使用該發現密鑰加密該直接通信請求以提供一經加密直接通信請求；及

傳輸該經加密直接通信請求。

【請求項3】

如請求項1至2中任一項之方法，其進一步包括：

將用於發現之一密鑰請求訊息傳輸(701)至與該遠端通信裝置相關聯之一應用功能節點(AF-1)，用於發現之該密鑰請求訊息包含一中繼服務碼；及

將用於通信之一密鑰請求訊息傳輸(705)至與該遠端通信裝置相關聯之該應用功能節點(AF-1)，用於通信之該密鑰請求訊息包含該中繼服務碼，

其中接收該發現密鑰包括：

從與該遠端通信裝置相關聯之該應用功能節點(AF-1)接收包含該發現密鑰之用於發現之一密鑰回應訊息，用於發現之該密鑰回應訊息與用於發現之該密鑰請求訊息相關聯，及

其中接收該通信密鑰及用於該通信密鑰之該密鑰ID包括：

接收包含該通信密鑰及用於該通信密鑰之該密鑰ID之用於通信之一密鑰回應訊息，用於通信之該密鑰回應訊息與用於通信之該密鑰請求訊息相關聯。

【請求項4】

如請求項3之方法，其進一步包括：

獲得(700)與該遠端通信裝置相關聯之該應用功能節點(AF-1)之一位址，

其中基於與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於發現之該密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)，及

其中基於與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於通信之該密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)。

【請求項5】

如請求項4之方法，其中獲得該位址包括從與該遠端通信裝置相關聯

之一直接發現名稱管理功能DDNMF節點提取與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址。

【請求項6】

如請求項4之方法，其中該直接通信請求包含與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址。

【請求項7】

如請求項3之方法，其中該直接通信請求包含該中繼服務碼。

【請求項8】

如請求項3之方法，其中該AF-1包括一近接服務密鑰管理功能PKMF。

【請求項9】

如請求項1至2中任一項之方法，其中該經加密發現訊息包括由該中繼通信裝置廣播之一經加密發現通告訊息。

【請求項10】

如請求項1至2中任一項之方法，其中發現該中繼通信裝置包括傳輸基於該發現密鑰加密之一經加密發現請求訊息，該經加密發現訊息包括對應於該經加密發現請求訊息之一經加密發現回應訊息，且使用該發現密鑰解密該經加密發現回應訊息。

【請求項11】

如請求項1至2中任一項之方法，其進一步包括使用該通信密鑰提供(717)與一無線電存取網路RAN節點之通信，與該RAN節點之該通信係透過該中繼通信裝置中繼。

【請求項12】

如請求項11之方法，其中提供該通信包括：

使用該發現密鑰加密該通信以提供一經加密通信；及

將該經加密通信傳輸至該中繼通信裝置。

【請求項13】

如請求項11之方法，其中提供該通信包括：

從該中繼通信裝置接收一經加密通信；及

使用該通信密鑰解密該經加密通信以提供來自該RAN節點之該通信。

【請求項14】

一種操作一中繼通信裝置之方法，該方法包括：

接收(808)一發現密鑰；

傳輸(809)一經加密發現訊息，使用該發現密鑰加密該經加密發現訊息；

從一遠端通信裝置接收(810)一直接通信請求，該直接通信請求包含一密鑰識別符ID；

獲得(811)對應於來自該直接通信請求之該密鑰ID之一通信密鑰；及

將一經加密直接通信回應傳輸(815)至該遠端通信裝置，使用對應於該密鑰ID之該通信密鑰加密該經加密直接通信回應。

【請求項15】

如請求項14之方法，其中接收該直接通信請求包括：

接收一經加密直接通信請求；及

使用該發現密鑰解密該經加密直接通信請求以提供該直接通信請求。

【請求項16】

如請求項14至15中任一項之方法，其進一步包括：

將用於發現之一密鑰請求訊息傳輸(807)至與該中繼通信裝置相關聯之一應用功能節點(AF-2)，該密鑰請求訊息包含一中繼服務碼，

其中接收該發現密鑰包括從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收包含該發現密鑰之用於發現之一密鑰回應訊息，用於發現之該密鑰回應訊息與用於發現之該密鑰請求訊息相關聯。

【請求項17】

如請求項16之方法，其進一步包括：

獲得(800)與該中繼通信裝置相關聯之該應用功能節點(AF-2)之一位址，

其中基於與該中繼通信裝置相關聯之該應用功能節點(AF-2)之該位址將用於發現之該密鑰請求訊息傳輸至與該中繼通信裝置相關聯之該應用功能節點(AF-2)。

【請求項18】

如請求項17之方法，其中獲得該位址包括從與該中繼通信裝置相關聯之一直接發現名稱管理功能DDNMF節點提取與該中繼通信裝置相關聯之該應用功能節點(AF-2)之該位址。

【請求項19】

如請求項16之方法，其中該直接通信請求包含該中繼服務碼。

【請求項20】

如請求項16之方法，其中該直接通信請求包含與該遠端通信裝置相關聯之一應用功能節點(AF-1)之一位址。

【請求項21】

如請求項20之方法，其中獲得該通信密鑰包括：

回應於接收到該直接通信訊息而將用於通信之一密鑰請求訊息傳輸至與該中繼通信裝置相關聯之該應用功能節點(AF-2)，用於通信之該密鑰請求訊息包含該密鑰ID及與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址；及

從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收用於通信之一密鑰回應訊息，該密鑰回應訊息包含對應於該密鑰ID之該通信密鑰。

【請求項22】

如請求項20之方法，其中獲得該通信密鑰包括：

回應於接收到該直接通信訊息而使用與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該位址將用於通信之一密鑰請求訊息傳輸至與該遠端通信裝置相關聯之該應用功能節點(AF-1)，用於通信之該密鑰請求訊息包含該密鑰ID；及

從與該遠端通信裝置相關聯之該應用功能節點(AF-1)接收用於通信之一密鑰回應訊息，該密鑰回應訊息包含對應於該密鑰ID之該通信密鑰。

【請求項23】

如請求項16之方法，其中該應用功能節點(AF-2)包括一近接服務密鑰管理功能PKMF。

【請求項24】

如請求項14至15中任一項之方法，其中該經加密發現訊息包括由該中繼通信裝置廣播之一經加密發現通告訊息。

【請求項25】

如請求項14至15中任一項之方法，其進一步包括接收一經加密發現請求訊息，

其中接收該經加密發現請求訊息包含使用發現密鑰解密該經加密發現請求訊息，

其中該經加密發現訊息包括回應於該經加密發現請求訊息而傳輸之一經加密發現回應訊息，且

其中使用該發現密鑰加密該經加密發現回應訊息。

【請求項26】

如請求項14至15中任一項之方法，其進一步包括：

使用用於在該遠端通信裝置與該中繼通信裝置之間加密之該通信密鑰中繼(817)該遠端通信裝置與一無線電存取網路RAN節點之間的通信，

其中中繼該通信包括以下之至少一者：

從該遠端通信裝置接收作為一經加密通信之該通信，使用該通信密鑰解密該經加密通信，且將該通信傳輸至該RAN節點；及

從該RAN節點接收該通信，使用該通信密鑰加密該通信以提供一經加密通信，且將該經加密通信傳輸至該遠端通信裝置。

【請求項27】

一種操作與一遠端通信裝置相關聯之一應用功能節點(AF-1)之方法，該方法包括：

從該遠端通信裝置接收(901)用於發現之一密鑰請求訊息，其中該密鑰請求訊息包含一中繼服務碼；

基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得(902)一發現密鑰；及

將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸(904)至該遠端通信裝置。

【請求項28】

如請求項27之方法，其中獲得該發現密鑰包括基於該中繼服務碼在內部導出該發現密鑰。

【請求項29】

如請求項27之方法，其中獲得(902)該發現密鑰包括，

回應於接收到用於發現之該密鑰請求訊息而將一密鑰請求訊息傳輸至與一中繼通信裝置相關聯之一應用功能節點(AF-2)，該密鑰請求訊息包含該中繼服務碼；及

從與該中繼通信裝置相關聯之該應用功能節點(AF-2)接收一密鑰回應訊息，該密鑰回應訊息包含該發現密鑰，

其中傳輸該密鑰請求訊息包括轉發用於發現之該密鑰請求訊息，且

其中傳輸用於發現之該密鑰回應訊息包括轉發該密鑰回應訊息。

【請求項30】

如請求項27至29中任一項之方法，其進一步包括：

從該遠端通信裝置接收(905a)用於通信之一密鑰請求訊息，用於通信之該密鑰請求訊息包含該中繼服務碼；

基於該中繼服務碼獲得(905b)一通信密鑰及用於該通信密鑰之一密鑰識別符ID；

將用於通信之一密鑰回應訊息傳輸(906)至該遠端通信裝置，該密鑰回應訊息包含該通信密鑰及用於該通信密鑰之該密鑰ID；

接收(912)一密鑰請求訊息，該密鑰請求訊息包含該密鑰ID；及

回應於接收到包含該密鑰ID之該密鑰請求訊息而傳輸(913)包含該通信密鑰之一密鑰回應訊息。

【請求項31】

一種操作與一中繼通信裝置相關聯之一應用功能節點(AF-2)之方法，該方法包括：

從該中繼通信裝置接收(1007a)用於發現之一密鑰請求訊息，該密鑰請求訊息包含一中繼服務碼；

基於包含於用於發現之該密鑰請求訊息中之該中繼服務碼獲得(1007b)一發現密鑰；及

將包含該發現密鑰之用於發現之一密鑰回應訊息傳輸(1008)至該中繼通信裝置。

【請求項32】

如請求項31之方法，其中獲得該發現密鑰包括基於該中繼服務碼在內部導出該發現密鑰。

【請求項33】

如請求項31至32中任一項之方法，其進一步包括：

從與該遠端通信裝置相關聯之一應用功能節點(AF-1)接收(1002a)一密鑰請求訊息，該密鑰請求訊息包含該中繼服務碼；及

基於包含於來自與該遠端通信裝置相關聯之該應用功能節點(AF-1)之該密鑰請求訊息中之該中繼服務碼獲得(1002b)該發現密鑰；

將包含該發現密鑰之一密鑰回應訊息傳輸(1003)至與該遠端通信裝置相關聯之該應用功能節點(AF-1)；

從該中繼通信裝置接收(1011)用於通信之一密鑰請求訊息，用於通信

之該密鑰請求訊息包含一密鑰識別符ID；

將包含該密鑰ID之一密鑰請求訊息傳輸(1012)至與一遠端通信裝置相關聯之一應用功能(AF-1)；

接收(1013)包含對應於該密鑰ID之一通信密鑰之一密鑰回應訊息，該密鑰回應訊息對應於該密鑰請求訊息；及

回應於接收到該密鑰回應訊息而將包含該通信密鑰之用於通信之一密鑰回應訊息傳輸(1014)至該中繼通信節點，

其中傳輸該密鑰請求訊息包括轉發用於通信之該密鑰請求訊息，且

其中傳輸用於通信之該密鑰回應訊息包括轉發該密鑰回應訊息。

【請求項34】

一種用於無線通信之實體(400、600、AF-1、AF-2)，其包括：

處理電路(403、603)；及

記憶體(405、605)，其與該處理電路耦合，其中該記憶體包含當由該處理電路執行時導致該實體執行如請求項1至33中任一項之操作之指令。

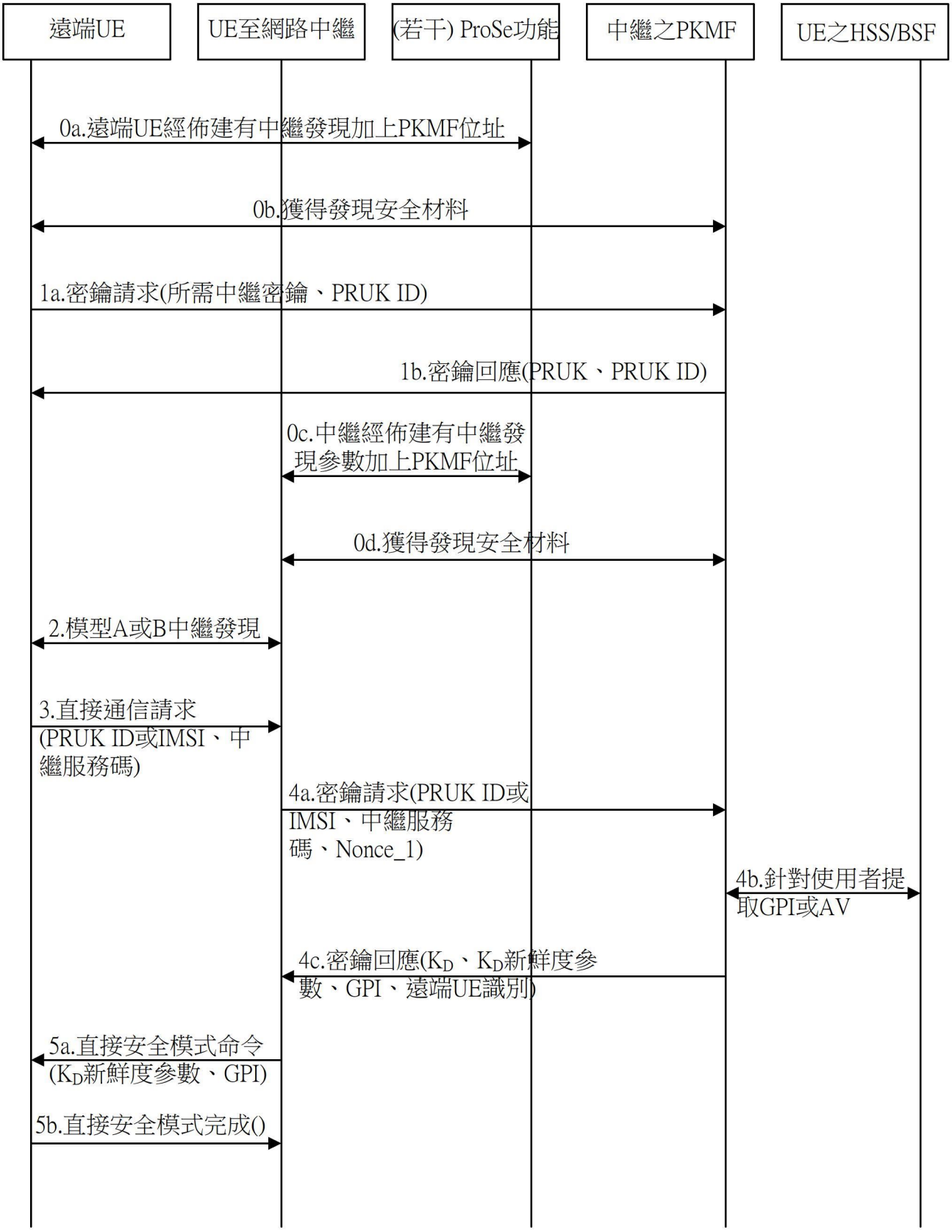
【請求項35】

一種電腦程式，其包括待由一實體(400、600、AF-1、AF-2)之處理電路(403、603)執行之程式碼，藉此該程式碼之執行導致該實體執行如請求項1至33中任一項之操作。

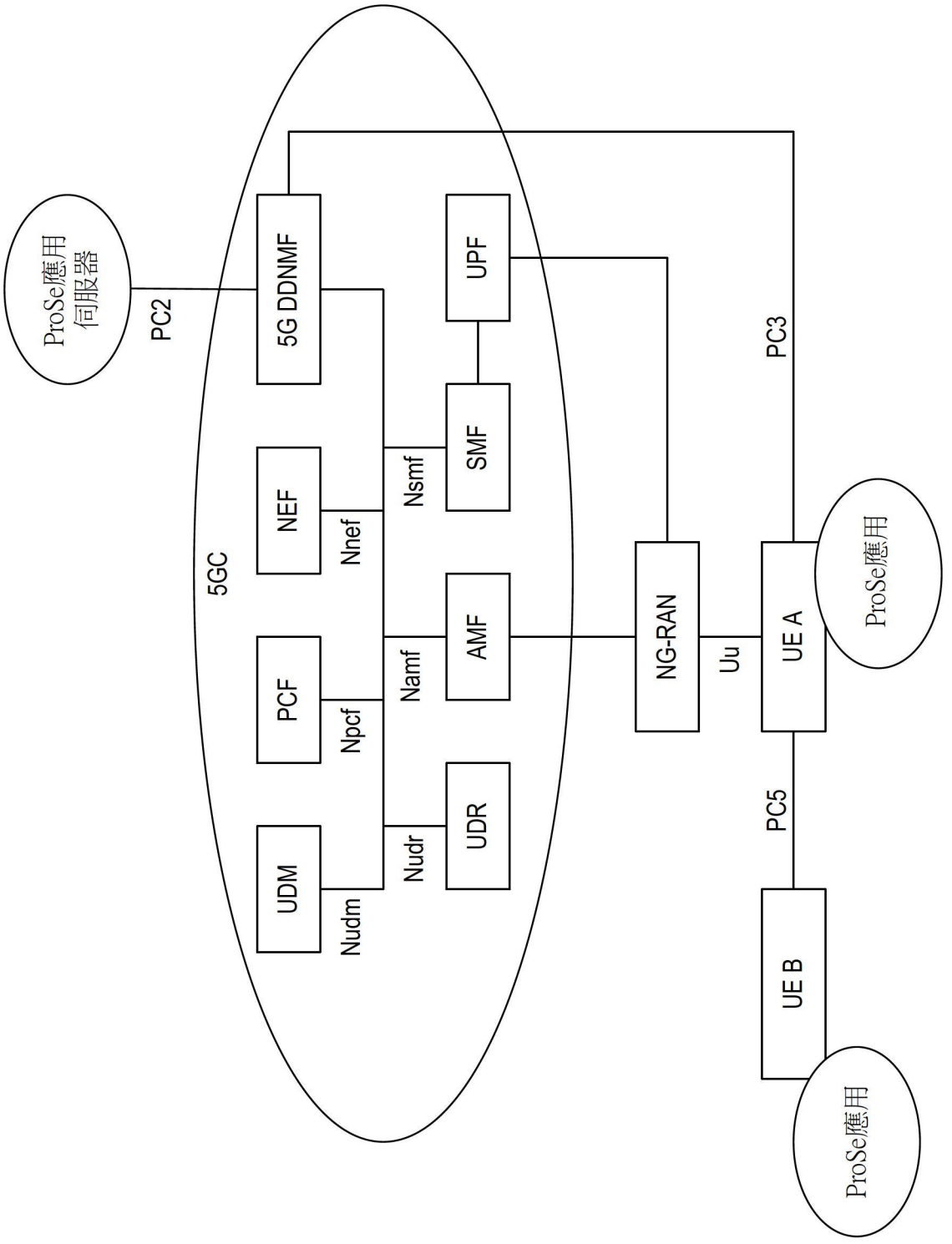
【請求項36】

一種電腦程式產品，其包括一非暫時性儲存媒體，該非暫時性儲存媒體包含待由一實體(400、600、AF-1、AF-2)之處理電路(403、603)執行之程式碼，藉此該程式碼之執行導致該實體執行如請求項1至33中任一項之操作。

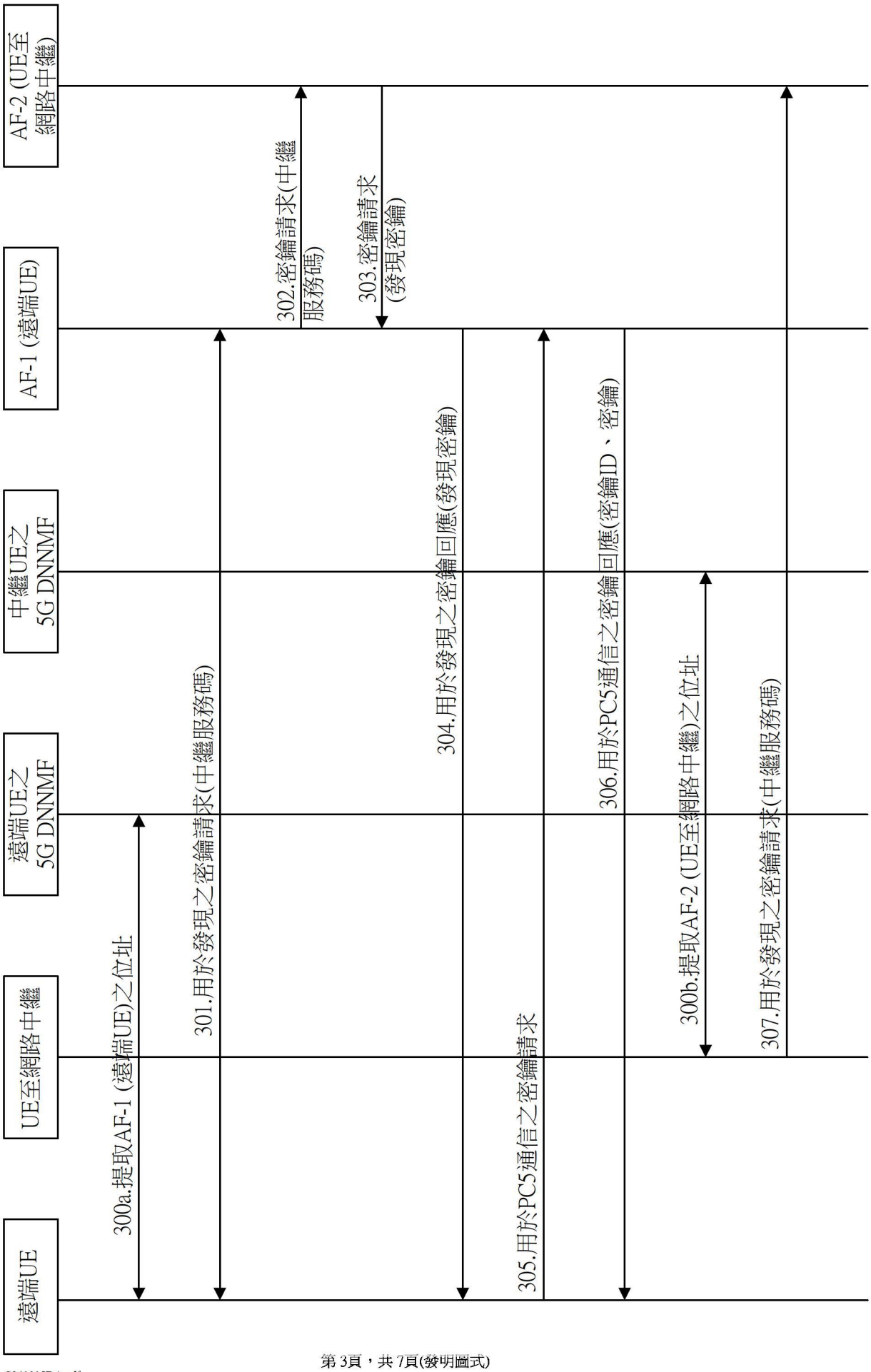
【發明圖式】


遠端UE
UE至網路中繼
(若干) ProSe功能
中繼之PKMF
UE之HSS/BSF
0a.遠端UE經佈建有中繼發現加上PKMF位址
0b.獲得發現安全材料
1a.密鑰請求(所需中繼密鑰、PRUK ID)
1b.密鑰回應(PRUK、PRUK ID)
0c.中繼經佈建有中繼發現參數加上PKMF位址
0d.獲得發現安全材料
2.模型A或B中繼發現
3.直接通信請求(PRUK ID或IMSI、中繼服務碼)
4a.密鑰請求(PRUK ID或IMSI、中繼服務碼、Nonce_1)
4b.針對使用者提取GPI或AV
4c.密鑰回應(K_D、K_D新鮮度參數、GPI、遠端UE識別)
5a.直接安全模式命令(K_D新鮮度參數、GPI)
5b.直接安全模式完成()

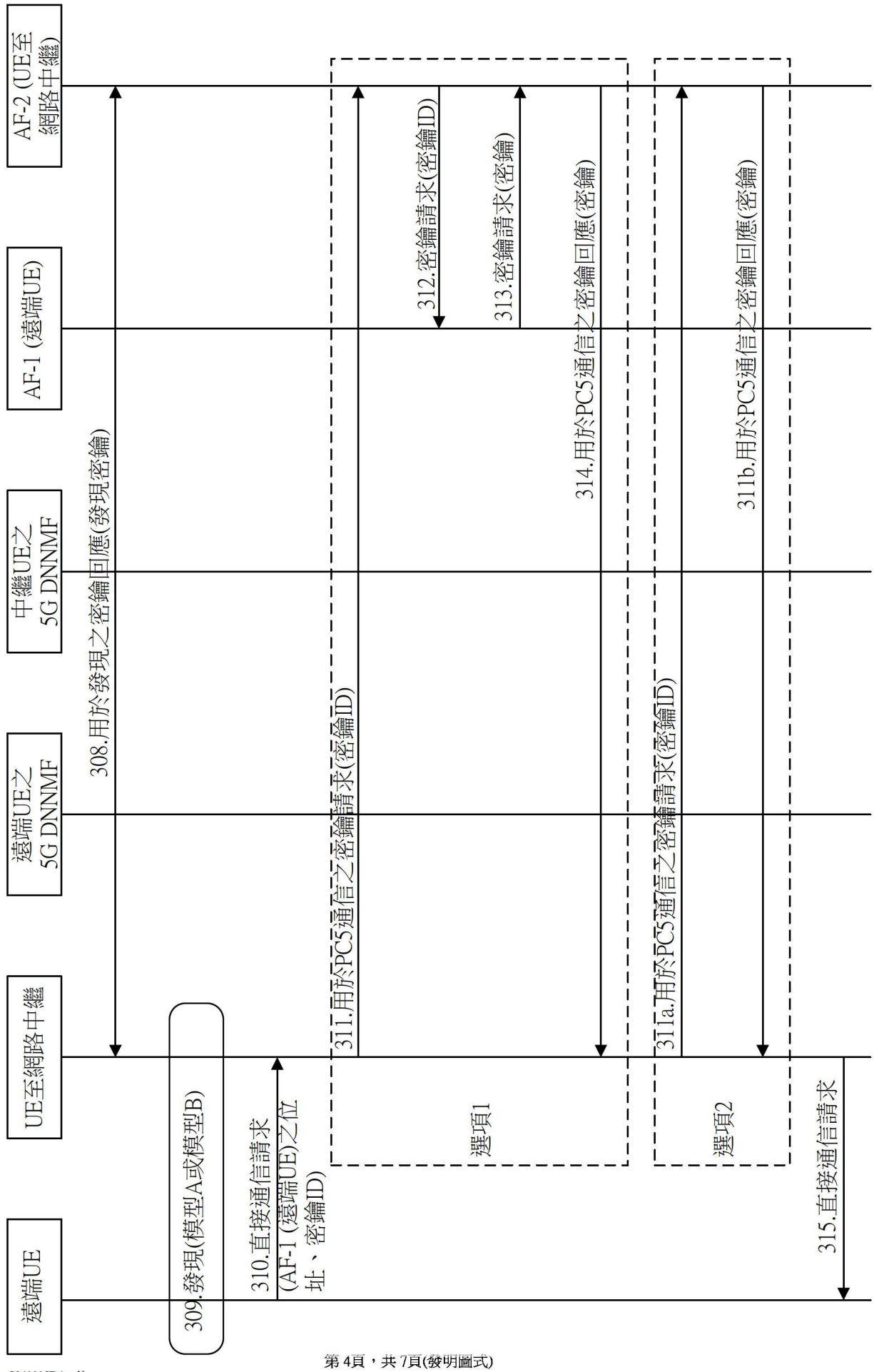
【圖1】


ProSe應用伺服器
PC2
5G DDNMF
5GC
NEF
PCF
UDM
Nnef
Npcf
Nudm
Nsmf
Namf
Nudr
SMF
AMF
UDR
UPF
NG-RAN
Uu
PC3
UE A
ProSe應用
PC5
UE B
ProSe應用

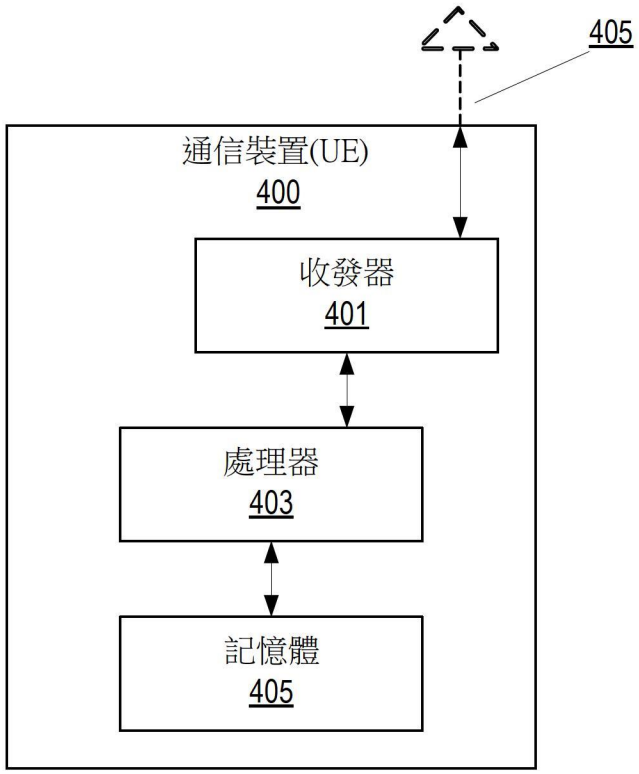
【圖2】


遠端UE
UE至網路中繼
遠端UE之 5G DNNMF
中繼UE之 5G DNNMF
AF-1 (遠端UE)
AF-2 (UE至網路中繼)
300a.提取AF-1 (遠端UE)之位址
301.用於發現之密鑰請求(中繼服務碼)
302.密鑰請求(中繼服務碼)
303.密鑰請求(發現密鑰)
304.用於發現之密鑰回應(發現密鑰)
305.用於PC5通信之密鑰請求
306.用於PC5通信之密鑰回應(密鑰ID、密鑰)
300b.提取AF-2 (UE至網路中繼)之位址
307.用於發現之密鑰請求(中繼服務碼)

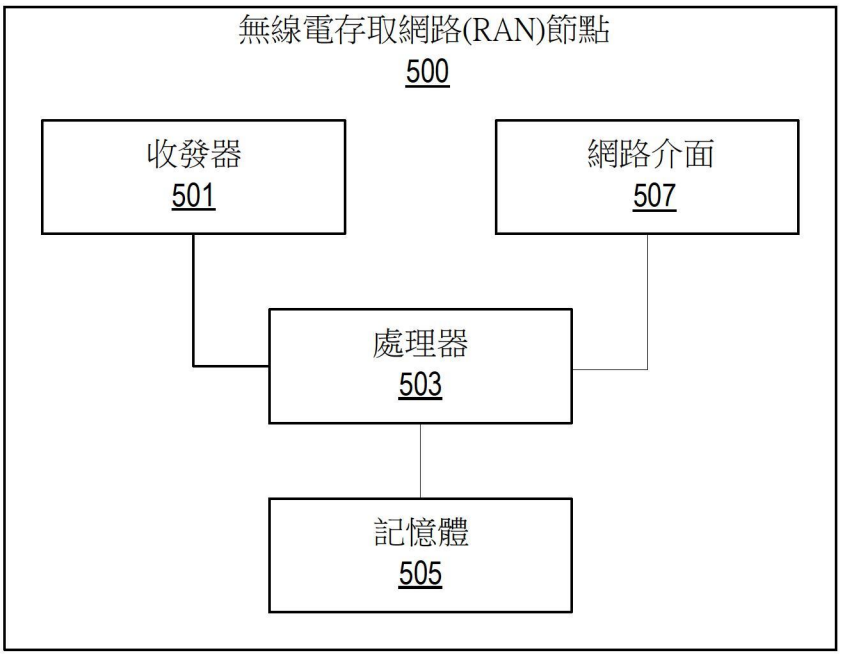
【圖3A】


遠端UE
UE至網路中繼
遠端UE之 5G DNNMF
中繼UE之 5G DNNMF
AF-1 (遠端UE)
AF-2 (UE至網路中繼)
308.用於發現之密鑰回應(發現密鑰)
309.發現(模型A或模型B)
310.直接通信請求 (AF-1 (遠端UE)之位址、密鑰ID)
311.用於PC5通信之密鑰請求(密鑰ID)
312.密鑰請求(密鑰ID)
313.密鑰請求(密鑰)
314.用於PC5通信之密鑰回應(密鑰)
選項1
311a.用於PC5通信之密鑰請求(密鑰ID)
311b.用於PC5通信之密鑰回應(密鑰)
選項2
315.直接通信請求

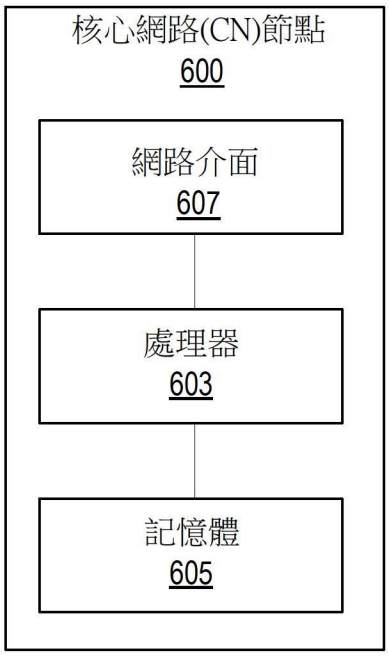
【圖3B】


405
通信裝置(UE)
400
收發器
401
處理器
403
記憶體
405

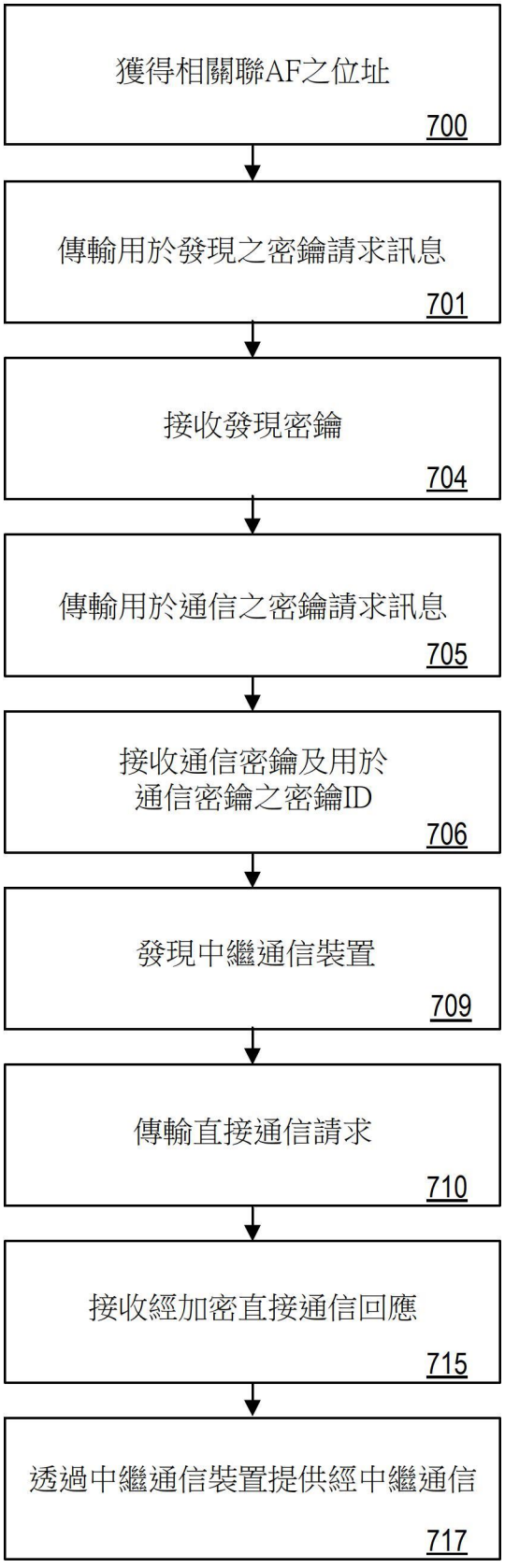
【圖4】


無線電存取網路(RAN)節點
500
收發器
501
網路介面
507
處理器
503
記憶體
505

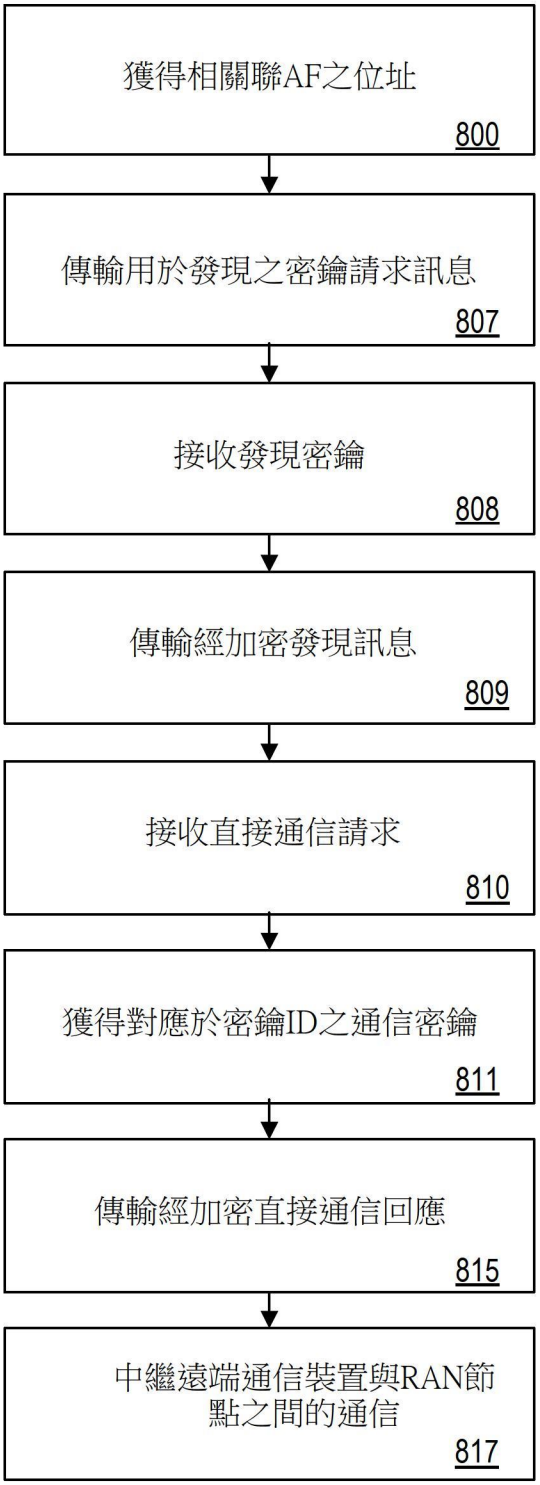
【圖5】


核心網路(CN)節點
600
網路介面
607
處理器
603
記憶體
605

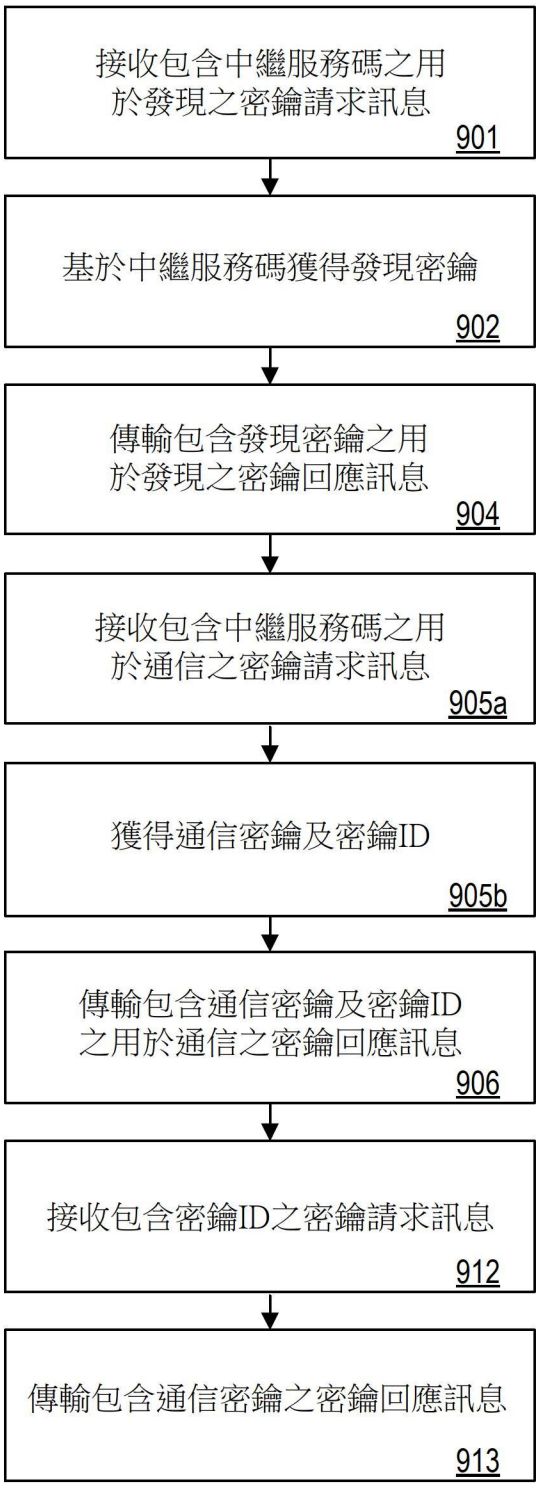
【圖6】


獲得相關聯AF之位址
700
傳輸用於發現之密鑰請求訊息
701
接收發現密鑰
704
傳輸用於通信之密鑰請求訊息
705
接收通信密鑰及用於通信密鑰之密鑰ID
706
發現中繼通信裝置
709
傳輸直接通信請求
710
接收經加密直接通信回應
715
透過中繼通信裝置提供經中繼通信
717

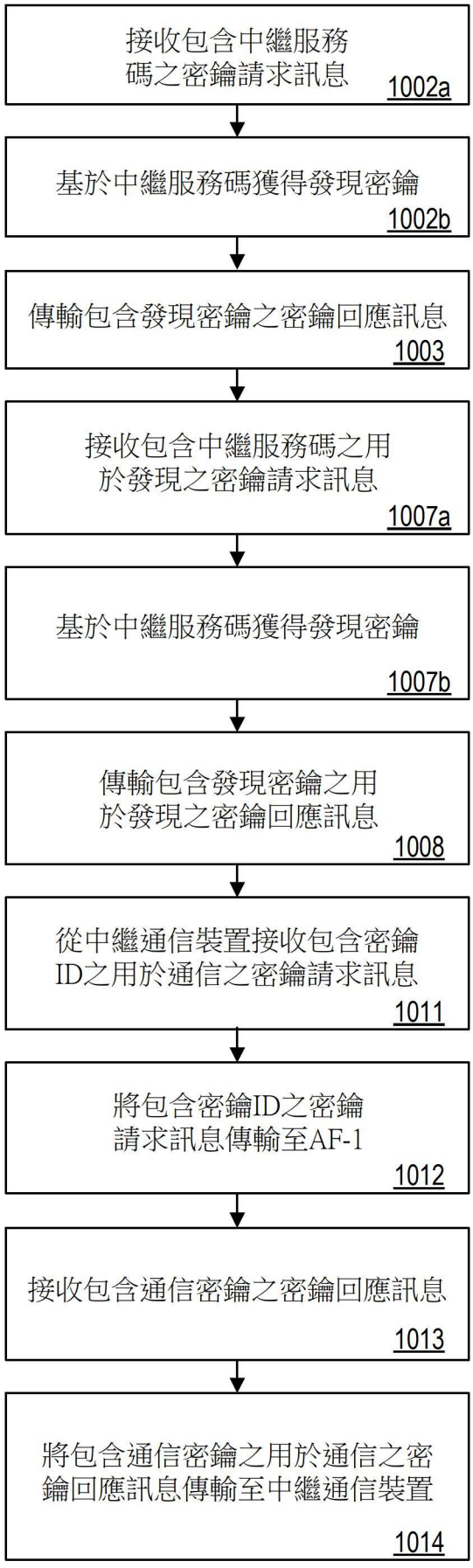
【圖7】


獲得相關聯AF之位址
800
傳輸用於發現之密鑰請求訊息
807
接收發現密鑰
808
傳輸經加密發現訊息
809
接收直接通信請求
810
獲得對應於密鑰ID之通信密鑰
811
傳輸經加密直接通信回應
815
中繼遠端通信裝置與RAN節點之間的通信
817

【圖8】


接收包含中繼服務碼之用於發現之密鑰請求訊息
901
基於中繼服務碼獲得發現密鑰
902
傳輸包含發現密鑰之用於發現之密鑰回應訊息
904
接收包含中繼服務碼之用於通信之密鑰請求訊息
905a
獲得通信密鑰及密鑰ID
905b
傳輸包含通信密鑰及密鑰ID之用於通信之密鑰回應訊息
906
接收包含密鑰ID之密鑰請求訊息
912
傳輸包含通信密鑰之密鑰回應訊息
913

【圖9】


接收包含中繼服務碼之密鑰請求訊息
1002a
基於中繼服務碼獲得發現密鑰
1002b
傳輸包含發現密鑰之密鑰回應訊息
1003
接收包含中繼服務碼之用於發現之密鑰請求訊息
1007a
基於中繼服務碼獲得發現密鑰
1007b
傳輸包含發現密鑰之用於發現之密鑰回應訊息
1008
從中繼通信裝置接收包含密鑰ID之用於通信之密鑰請求訊息
1011
將包含密鑰ID之密鑰請求訊息傳輸至AF-1
1012
接收包含通信密鑰之密鑰回應訊息
1013
將包含通信密鑰之用於通信之密鑰回應訊息傳輸至中繼通信裝置
1014

【圖10】