

申請日期	91.5.31
案 號	91111721
類 別	H40 7/20

A4

C4

(以上各欄由本局填註)

發明專利說明書

一、發明 新 名稱	中 文	無線環境中之安全應用散發及執行
	英 文	SAFE APPLICATION DISTRIBUTION AND EXECUTION IN A WIRELESS ENVIRONMENT
二、發明 創作 人	姓 名	1.勞倫斯 朗布雷 LAURENCE LUNDBLADE 2.馬克 S. 菲利普 MARC S. PHILLIPS 3.布萊恩 米尼爾 BRIAN MINEAR
	國 籍	1.-3.均美國 U.S.A.
三、申請人	住、居所	1.美國加州聖地牙哥市那夫加塔克街3062號 3062 NAVGATUCK, SAN DIEGO, CALIFORNIA 92117, U.S.A. 2.美國加州聖地牙哥市葛洛斯范特道4008號 4008 GROS VENTRE AVENUE, SAN DIEGO, CALIFORNIA 92117, U.S.A. 3.美國加州聖地牙哥市馮塔尼里廣場13704號 13704 FONTANELLE PLACE, SAN DIEGO, CALIFORNIA 92128, U.S.A.
	姓 名 (名 稱)	美商奎康公司 QUALCOMM INCORPORATED
	國 籍	美國 U.S.A.
	住、居所 (事務所)	美國加州聖地牙哥市摩豪斯大道5775號 5775 MOREHOUSE DRIVE, SAN DIEGO, CALIFORNIA 92121-1714, U.S.A.
	代 表 人 姓 名	菲力普 R. 華德渥斯 PHILIP R. WADSWORTH

申請日期	
案 號	
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	
	英 文	
二、發明 人	姓 名	4.宋研 YAN ZHUANG 5.亞那德 克里希南 ANAND KRISHNAN 6.史帝芬 A. 斯普里吉 STEPHEN A. SPRIGG
	國 籍	4.中國 CHINA 5.印度 INDIA 6.美國 U.S.A.
	住、居所	4.美國加州聖地牙哥市傑寇斯路8223號 8223 JADE COAST ROAD, NO. 120, SAN DIEGO, CALIFORNIA 92126, U.S.A. 5.美國加州聖地牙哥市梭布尼巷13775號 13775 SORBONNE COURT, SAN DIEGO, CALIFORNIA 92128 U.S.A. 6.美國加州波威市崔佛丁巷12124號 12124 TRAVERTINE COURT, POWAY, CALIFORNIA 92064, U.S.A.
	姓 名 (名 稱)	
三、申請人	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝
訂
線

申請日期	
案 號	
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明名稱	中 文	
	英 文	
二、發明人	姓 名	7.馬森 克梅特里 9.葛拉德 豪爾 MAZEN CHMAYTELLI GERALD HOREL 8.米榭爾 奧立佛 MITCHELL OLIVER
	國 籍	7.黎巴嫩 LEBANON 8.美國 U.S.A. 9.加拿大 CANADA
	住、居所	7.美國加州聖地牙哥市林伍街1752號 1752 LINWOOD STREET, NO. G, SAN DIEGO, CALIFORNIA 92110, U.S.A. 8.美國加州聖地牙哥市卡米尼圖街9737號 9737 CAMINITO SUELTO, SAN DIEGO, CALIFORNIA 92131, U.S.A. 9.加拿大英屬哥倫比亞省布蘭特伍灣市托林路6500號 6500 TORIN ROAD, BRENTWOOD BAY, BRITISH COLUMBIA V8M2H5, CANADA
	姓 名 (名 稱)	
三、申請人	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝
訂
線

申請日期	
案 號	
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 新型名稱	中 文	
	英 文	
二、發明 創作人	姓 名	10.卡倫 克洛斯蘭 KAREN CROSSLAND
	國 籍	10.美國 U.S.A.
	住、居所	10.美國加州聖地牙哥市梅那街5044號 5044 MAYNARD STREET, SAN DIEGO, CALIFORNIA 92122, U.S.A.
三、申請人	姓 名 (名 稱)	
	國 籍	
	住、居所 (事務所)	
	代 表 人 姓 名	

裝
訂
線

(由本局填寫)

承辦人代碼：
大類：
I P C 分類：

A6

B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權
美國 2001年05月31日 09/872,418 ☒有 ☐無主張優先權

有關微生物已寄存於：

寄存日期：

，寄存號碼：

裝

訂

線

五、發明說明 ()

發明領域

本發明與處理一無線裝置中使用的應用有關，尤其本發明與增強一無線裝置上執行之應用的安全性、安全及完整性有關。

發明背景

近年來，無線通信已面臨爆發性成長。隨著消費者及商業愈來愈依據無線裝置(如行動電腦、個人數位助理(PDA))，無線服務提供者(電信業者)致力於在這些無線裝置上提供額外功能。這項額外功能不僅會增加無線裝置需求，而且還會增加現有使用者的使用量。但是，增加功能(特別是增加無線裝置可存取之應用的功能)會提高成本及複雜度，促使電信業者放棄這項功能。

另外，有一點無法保證當將應用安裝在無線裝置上時，會正確執行應用。目前，信賴應用在無線裝置上執行的能力得依靠開發者、無線裝置製造業者及/或電信業者。隨著開發出更多應用及無線裝置上的應用數量遞增，無線裝置環境變得愈來愈動態。例如，在任何給定時間，無線裝置可從大量可用的應用中選擇要擷取或執行數個不同的應用。因此，確保將任何給定的應用散發至無線裝置及安全執行變得更難以控制。

這屬於特別重要事項，因為不適當執行應用不僅會對無線裝置造成不利的影響，而且還可能危及電信業者網路及其他網路組件，包括其他無線裝置。例如，如果在不受限制情況下，應用可控制無線裝置的功率控制，並且造成其他無

五、發明說明(2)

線裝置之間的干擾，以及伺服該無線裝置之細胞中的整體容量。

目前，無線裝置製造商及電信業者都不支援在動態應用散發及執行環境中測試及安全散發應用。因此，會顧慮散發及在無線裝置上執行的應用會危及無線裝置、電信業者網路或其他網路組件。

此外，隨著開發出更多應用及用於將應用傳輸至無線裝置的環境變得更動態，會引發其他安全問題。隨著應用數量及創作這些應用的開發者數量遞增，對知道任何給定應用來源(即，開發者)的渴望也遞增。在某種可靠度程度內，電信業者或手機製造商想要知道可決定應用來源，以防萬一應用會造成危害。

於是，本技藝中需要一種用於提供在一無線裝置上散發及執行應用之更安全環境的系統及方法。

發明概要

根據本發明的系統及方法可克服現有系統的缺點，其方式為建立用於應用散發及執行的安全環境，該安全環境以預先決定標準測試應用、為開發者提供不拒絕的追蹤能力、檢查應用是否有被非預定修改、允許從無線裝置移除應用，及/或使用用於定義可執行應用之環境的規則及使用權限。

認證應用符合預先決定標準的優點為，可預先捕捉會於執行期間發生的可能錯誤。這有助於防止應用執行的有害影響。

追蹤能力的優點為不拒絕。如果應用有任何問題，則追溯

五、發明說明 (3)

應用來源(即，開發者)有助於校正問題。此外，追蹤能力阻止開發者建立具有有害結果的應用，無論是否是故意。

另外，在無線裝置接收應用之前先決定應用是否被修改之功能的優點為，藉由確保所接收應用相同於所傳輸應用以增加安全性。由於在無線環境中會更自由散發應用，所以決定應用是否被修改的功能會增加無線裝置所接收的應用未被修改的可信度，無論是否是故意。

提供用於定義何時可執行應用的一組規則及使用權限也可增強應用散發及執行系統的安全，其方式是防止在平台(例如，未授權應用的系統或環境中)上未經授權執行應用。

從無線裝置移除應用的功能也增強應用散發系統的安全。如果將應用安裝在手機上，無論是由製造商或透過應用下載，都具有一種移除應用的機制，因為藉由移除可能有害及不要的程式碼，預料之外的負面結果增加應用散發及執行系統的安全。

根據本發明的系統及方法可叫用(invoké)本文中說明的一個或一個以上技術。但是，藉由叫用本文中揭示及提出的所有技術，根據本發明的系統及方法提供高品質及安全的應用散發及執行。

在本發明具體實施例中，本發明揭示一種用於散發及處理一應用之方法，該方法包括下列步驟：接收該應用及識別資訊；認證該應用符合一預先決定準則；將一使用權限指派給該應用；使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置；決定於傳輸期間該應用是否有被

五、發明說明 (4)

修改；在該裝置上儲存一規則；使用該使用權限及該規則來決定是否可處理該應用；以及從該裝置移除該應用。

在本發明另一項具體實施例中，本發明揭示一種在一無線裝置上執行一應用之方法，該方法包括下列步驟：儲存一用於評估一使用權限的規則；使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；接收一用於在該無線裝置上執行該應用的要求；評估該所接收資訊以決定該所接收資訊是否有被修改；如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及如果授予該使用權限，則執行該應用。

在本發明尚有另一項具體實施例中，本發明揭示一種在一無線裝置上執行一應用之方法，該方法包括下列步驟：儲存一用於評估一使用權限的規則；使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；接收一用於在該無線裝置上執行該應用的要求；評估該所接收資訊以決定該所接收資訊是否有被修改；如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及如果授予該使用權限，則執行該應用。

圖式簡單說明

併入並建構說明書的一部份的附圖圖解說明本發明的目前較佳具體實施例，並且附圖連同前面的一般說明與下文中的較佳具體實施例詳細說明係用來解說本發明原理。圖式中：

圖1顯示用於解說本發明示範性具體實施例之安全應用散

五、發明說明(5)

發及執行之高階處理程序的流程圖；

圖2顯示可實施本發明示範性具體實施例之系統架構的方塊圖；

圖3顯示可實施根據本發明示範性具體實施例之安全應用散發處理系統之無線網路架構的方塊圖；

圖4顯示本發明示範性具體實施例之無線裝置及部份內部組件的方塊圖；

圖5顯示本發明示範性具體實施例之用於建立一數位簽名及傳輸至一無線裝置之資訊的方塊圖；

圖6顯示用於解說本發明示範性具體實施例之用於散發應用之伺服器使用之步驟的流程圖；以及

圖7顯示用於解說本發明示範性具體實施例之無線裝置執行應用時使用之步驟的流程圖。

較佳具體實施例詳細說明

現在將參考如附圖所示的本發明的示範性及較佳具體實施例詳細說明本發明，其中整份附圖中的相似的參照文字代表相似或對應的零件。熟知技藝人士細讀下文中參考附圖的詳細說明後，將可明白本發明的性質、目的及優點。

本發明揭示安全且牢靠的應用散發及執行，其方式提供應用測試系統及方法，以確保符合與應用執行環境相關的預先決定準則。另外，藉由使用規則與權限清單、應用移除及如數位簽名之類的修改偵測技術，本發明提供機制以安全散發及執行經過測試或未經測試應用，其方式為決定該應用是否已被修改、決定該應用是否具有在一給定無線裝

五、發明說明(6)

置環境中執行的權限，以及萬一希望移除該應用時移除該應用。

熟知技藝人士應明白，基於簡化說明目的，前面說明散發及執行應用檔案類型。“應用”還可包括具有可執行內容的檔案，如：物件程式碼、指令檔、java檔案、書籤檔案(或PQA檔案)、WML指令檔、位元組碼(byte code)及perl指令檔。此外，本文中提及的“應用”還可包括本質上不可執行的檔案，如需要開啟的文件或需要存取的其他資料檔案。

圖1顯示根據本發明示範性具體實施例之安全應用散發及執行之高階處理程序的流程圖。本發明具體實施例促使開發者識別能夠與應用關聯、針對預定執行應用的環境實施應用之測試、指派可用來指示哪一些裝置或系統可執行該應用的使用權限，以及一應用執行非法或非期望動作時移除該應用。

系統及方法最好採用所有這些技術，以增強應用之安全散發及執行。但是，應明白，甚至採用所有這些技術的一項或一項以上技術仍然可增強應用之安全散發及執行。

高階處理程序以使開發者識別與應用關聯開始(步驟100)。可藉由當散發應用時繫結開發者識別與應用來執行這項處理程序。或者，可將開發者識別連同對應應用一起儲存在系統中的伺服器上。最好也儲存開發者識別資訊，並且與應用資訊關聯，以便無法很容易修改資訊。

然後測試應用是否有不適當的作業(步驟105)。在環境中使用不適當作業的應用不僅會影響執行應用的環境，而且還

五、發明說明 (7)

會影響連接至該裝置或透過網路連接至該裝置的其他裝置。最好測試應用，使應用不能進行不適當的系統呼叫，或是於應用作業期間對裝置或其他連接裝置造成負面影響。在一項具體實施例中，這項測試係藉由一認證處理程序來執行，其中會測試應用以決定該應用是否符合預先決定準則。最好使用與開發者無關的認證處理程序來執行應用。獨立的認證處理程序有助於更精確且可靠測試。

執行應用之前，先檢查應用以決定該應用是否「被允許」在裝置上執行(步驟110)。可藉由使用如下文所述的使用權限及規則來執行檢查，或藉由熟知技藝人士已知的其他使用權限機制。另外，最好在嘗試執行應用之前，先檢查應用。這項反覆檢查處理程序增強執行應用的安全性。例如，可防範具有已經由另一應用而插入在執行中裝置上之應用的Trojan horse的應用。

然後，移除裝置中執行不適當或非預期作業的應用(步驟115)。這可防止應用進行任何進一步破壞，並且也釋出裝置中的記憶體以供其他用途之用。或者，不需要從裝置移除應用。移除應用可表示停用應用，以及結束裝置上的應用。

圖2顯示可實施本發明示範性具體實施例的系統架構。開發者200建立用於在無線裝置230上使用的應用。如上文所述，熟知技藝人士應明白，雖然前面說明包括一種應用檔案類型，但是可使用其他檔案類型。另外，熟知技藝人士應明白，本發明可配合其他無線裝置或非無線裝置一起使用，並且可採用無線網路、非無線網路或其組合。

五、發明說明(8)

一般而言，開發者200具一組開發規格，用於開發在無線裝置230上執行的應用。在一項具體實施例中，無線裝置包括一軟體平台，用以輔助應用與無線裝置之間的介面，如總公司位於美國加州聖地牙哥QUALCOMM Incorporated公司開發的BREW™軟體。開發者可建立符合軟體平台或BREW™軟體、規格標準及慣例的應用。

在一項具體實施例中，開發者200被連接至中央伺服器205，以便可用電子方式將應用傳輸至中央伺服器205。在一項具體實施例中，中央伺服器是用於將應用散發至無線裝置的應用控制中心總部(Application Control Center Headquarters; ACCHQ)。開發者200可數位簽名應用(如上文所述)，以決定該應用是否有被修改。應明白，不需要實際連接至中央伺服器。例如，開發者200可經由優先投遞郵件將儲存在CD-ROM上的應用傳送至中央伺服器205。

此外，開發者將各種來源識別資訊傳送至中央伺服器205。這項來源識別資訊可包括與應用關聯之用於識別開發者的任何類型資訊，如公司名稱、公司稅金識別或其他識別資訊。

在分析及認證應用過程中會使用中央伺服器205本身或使用認證伺服器210。在一項具體實施例中，可使用應用控制中心(Application Control Center; ACC)當作認證伺服器。認證伺服器210可用來分析應用，以決定該應用是否符合預先決定認證準則。這項準則可包括該應用是否符合在一無線裝置或平台上執行的開發規則。但是，認證準則可能是應用必須

五、發明說明 (9)

先符合的任何準則，之後才能在一無線裝置或平台上執行。此類的準則可包括確認：(a)應用功能與開發者聲稱的功能，所以應用不會危及無線裝置的操作(例如，不會使手機當機)；(b)應用不能存取不應存取的資料或記憶體(例如，不能存取其他應用、作業系統或平台軟體所擁有的資料或檔案)；以及(c)不會對無線裝置資源造成負面影響，如有害地獨佔無線裝置的輸入及輸出。

中央伺服器205也會在一清單中指派與應用關聯的一組使用權限。這個使用權限清單係藉由各種因數決定，包括分析應用是否通過認證處理程序、准許在什麼網路220上執行應用，及無線裝置是否支援應用。當實施本發明時，可能有許多因數用於決定使用權限清單，並且由熟知技藝人士決定。

中央伺服器205接收開發者識別資訊，並且使開發者識別資訊與開發者200建立的應用互相關聯。萬一應用有任何問題，中央伺服器能夠識別應用來源。在一項具體實施例中，會將開發者資訊傳送給無線裝置230，以便由該無線裝置與連接至該無線裝置的執行互相關聯。

在一項具體實施例中，中央伺服器也被連接至應用下載伺服器(ADS)215。應用下載伺服器215係用來經由無線網路220連接無線裝置，以下載應用。中央伺服器也會將與應用關聯的使用權限清單及開發者識別傳送至ADS，以在傳輸至無線裝置之前，利用ADS儲存使用權限清單及開發者識別。應用、使用權限清單及開發者識別最好先經過中央伺服器的數位簽名，以增強防修改的安全性。

五、發明說明 (10)

熟知技藝人士應明白，ADS可用於連接至多重網路220，以將應用、檔案及其他資訊散發至各種無線裝置230。另外，可採用無線網路及非無線網路，以將應用的使用權限清單及開發者識別傳輸至無線裝置。

響應應用要求，ADS 215經由網路220將應用、使用權限清單、開發者識別及數位簽名傳輸至無線裝置230。在一項具體實施例中，無線裝置230包含用於檢查數位簽名的金鑰，以決定應用、使用權限清單及/或開發者識別是否有被修改。

如果在本發明中採用數位簽名，則中央伺服器最好使用一安全鑰來建立數位簽名，並且在無線裝置上安裝金鑰，以評估數位簽名。藉由使用安全鑰，無線裝置將具有較高的可靠度確定數位簽名係由中央伺服器所建立，而不是由冒充者建立。

萬一應用造成無線裝置發生錯誤，或基於任何其他期望的因素，無線裝置可起始移除該應用。另外，可依據來自於ADS或中央伺服器的要求，從無線裝置移除應用。可基於任何期望的因素，起始來自於伺服器的要求。例如，伺服器可起始從無線裝置移除應用，因為在另一裝置上不適當執行應用、散發新版本應用，或甚至指示應移除應用的商業因素。這項應用移除處理程序進一步防止無線裝置環境重新執行已損毀及/或破壞的應用。

圖3顯示可實施根據本發明示範性具體實施例之應用散發系統的無線網路架構。中央伺服器302是一種實體，其用途為藉由本身或結合認證伺服器以認證應用程式相容於程式

五、發明說明 (11)

設計標準或慣例。如上文所述，可建立這些程式設計標準，以在軟體平台(如 BREW™ 平台)上執行應用。

在一項具體實施例中，中央伺服器資料庫 304 係由在網路 300 中在任何時間下載至每個無線裝置 330 之每個應用程式的識別記錄、下載應用程式之個人的電子服務號碼(Electronic Service Number; ESN)與帶有該應用程式之無線裝置 330 的唯一行動識別號碼(Mobile Identification Number; MIN)所組成。或者，中央伺服器資料庫 304 含有無線裝置模型之網路 300 中每個無線裝置 330 的記錄、無線網者業者、使用無線裝置 300 之區域及有助於識別無線裝置 330 正確帶有哪一些應用程式的任何其他資訊。此外，中央伺服器資料庫也可儲存與應用關聯的開發者識別資訊。

在一項具體實施例中，中央伺服器 302 也可包括移除命令來源 322。移除命令來源 322 是可決定移除一個或一個以上目標應用程式的人或實體。移除命令來源 322 也是建構一移除命令 316 (如上文所述)的實體，該移除命令 316 會廣播至帶有目標應用程式的所識別無線裝置 330。或者，在沒有限制情況下，移除命令來源 322 可能是涉及開發與發佈目標應用程式的人或實體、涉及製造無線裝置 330 的人或實體及/或涉及網路 300 任一部份功能的人或實體。

中央伺服器 302 透過網路 308 (如最好是安全的網際網路)以與一個或一個以上電腦伺服器 306 (例如，ADS)通信。伺服器 306 也經由網路 308 與電信業者網路 310 通信。電信業者網路 310 係藉由網際網路及傳統舊式電話系統(Plain Ordinary Telephone

五、發明說明 (12)

System ; POTS)(圖 3 中共同標示為 311)與 MSC 312 通信。介於電信業者網路 310 與 MSC 312 之間的網際網路連接 311 傳遞資料，而 POTS 311 則是傳遞語音資訊。接著，MSC 312 被連接到多重基地台 (BTS) 314。MSC 312 係藉由網際網路 311 (用於傳遞資料) 及 POTS 311 (用於傳遞語音資訊) 連接至 BTS。BTS 314 藉由短傳訊服務 (short messaging service ; SMS) 或任何其他透過空間之方法，以無線方式將訊息傳送至無線裝置 330。

在本發明中，BTS 314 傳送之訊息的實例之一是移除命令 316。如本文中的進一步說明，無線裝置 330 響應接收到的移除命令 316，其響應方式是解除安裝儲存在無線裝置 330 上的目標應用程式。在一項具體實施例中，可額外或另外程式設計移除程式，以停用目標應用程式或重新程式設計目標應用程式以不同方式執行。無線裝置也可刪除應用及任何相關資訊，如使用權限清單。

移除命令 316 是由移除命令來源 322 (移除命令來源可能是決定起始移除目標應用程式的同一或不同人或實體) 建構而成。移除命令來源 322 透過網路 300 傳送移除命令 316，以廣播至無線裝置 330。

藉由使用前面具體實施例中說明的移除命令，由於提供解除安裝已損毀或非期望應用的機制，所以可增加應用散發及執行的安全性。熟知技藝人士應明白，雖然前面說明藉由中央伺服器起始移除命令，但是無線裝置也可起始移除或解除安裝應用及其相關資訊。

同樣地，前面的網路可用來透過 MSC 及 BTS 將應用、使用

五、發明說明 (13)

權限清單與相關數位簽名從中央伺服器傳送至各種伺服器330(例如, ADS⁷)。

圖4顯示本發明示範性具體實施例的無線裝置及部份內部組件。雖然本具體實施例係針對無線裝置400,但這是當作實例,而沒有任何預定的限制。或者,可在能夠透過網路通信的任何形式遠端模組來執行本發明,包括但不限於,無線裝置與非無線裝置,如個人數位助理(PDA)、無線數據機、PCMCIA卡、接取終端機、個人電腦、不含顯示器或鍵盤的裝置或其任何組合或子組合。這些示範性遠端模組也可具有使用者介面,如鍵盤、視覺顯示器或聲音顯示器。

圖4所示的無線裝置400具有製造無線裝置400時安裝的專用積體電路(application-specific integrated circuit; ASIC)415。ASIC是一種由包含於ASIC中的軟體所驅動的硬體組件。製造時,也會將應用程式設計介面(API)410安裝在無線裝置400中。在一項具體實施例中,API代表BREW API或軟體平台。API 410是一種被建置以與ASIC互動的軟體程式。API 410係當作安裝在無線裝置400上之ASIC 415硬體與應用程式(如上文所述)的介面。或者,無線裝置400可包含任何其他形式的電路元件,以允許程式以相容於無線裝置400硬體組態的方式運作。無線裝置400還具有儲存裝置405。儲存裝置405係由隨機存取記憶體(RAM)與唯讀記憶體(ROM)所組成,但是,或者可能是任何形式的記憶體,如插入的EPROM、EEPROM或快閃記憶卡。

無線裝置的儲存區405可用來儲存所接收應用及使用權限清單425。此外,儲存區405可用來儲存一個或一個以上「金

五、發明說明 (14)

鑰」405。可使用簽名演算法將這些金鑰套用至數位簽名，以決定有簽名的資訊是否有被修改。

規則435也可被安裝在無線裝置400上。這些規則可配合使用權限清單一起使用，以決定是否允許執行應用。例如，規則可陳述如果使用權限清單中的認證旗標被設定(例如，指示應用通過認證)，則允許執行應用。使用權限清單是否具有認證旗標設定取決於是否通過認證。藉由將規則套用至內含於使用權限清單中的資訊，以授予或拒絕執行應用的使用權限。

當製造無線裝置400時，無線裝置400製造商(圖中未顯示)可將應用程式下載至無線裝置400的儲存裝置405。這些應用程式可能是對無線裝置使用者可能有幫助或娛樂性的任何程式，如遊戲、書籍或是任何其他類型資料或軟體程式。製造無線裝置後，還可透過空氣將應用程式下載至無線裝置400。

當無線裝置400執行移除程式時，移除程式從儲存在無線裝置400上的應用程式之一解除安裝一個或一個以上目標應用程式。目標應用程式是基於下文中說明的各種原因而必須從無線裝置400解除安裝的應用程式。

無線裝置400具有製造商安裝的本機資料庫420。無線裝置的API被程式設計以使用關於儲存在無線裝置400上之每個應用程式的識別資訊的記錄來更新本機資料庫420。本機資料庫420包含儲存在無線裝置400上之每個應用程式的唯一簽名識別的記錄。此外，本機資料庫420還可包含位於無線裝置

五、發明說明 (15)

400上之儲存裝置405之應用程式位置的記錄，以及有助於持續追蹤無線裝置400上下載哪一些應用程式及其位置的任何其他資訊。

圖5顯示本發明示範性具體實施例之用於建立一數位簽名及傳輸至一無線裝置之資訊的方塊圖。如熟知技藝人士所知，數位簽名可用來追蹤數位檔案是否已被修改。如上文所述，數位簽名可被套用至任何數位檔案，包括文件、應用、資料庫等等。一般而言，數位簽名被建立的方式為，使用簽名演算法將金鑰套用至檔案。這個數位簽名係使用包含於檔案中的資訊所建立。通常會將數位簽名連同檔案一起傳送給收件人。然後，檔案及數位簽名收件人可將一金鑰套用至所接收檔案及數位簽名，以決定於傳輸至收件人期間檔案是否已被修改。

用來建立及評估數位簽名的金鑰可用來決定簽名者的身份。例如，一實體可產生金鑰以建立數位簽名並保持安全性。這個實體可散發用來評估數位簽名的對應金鑰。如果金鑰保持安全性並且未洩露，則評估數位簽名的收件人不僅可決定資訊是否已被修改，而且還可決定簽名者的身份。

或者，第三方實體可用安全方式來建立特定實體的金鑰。因此，具有與特定身份相關之金鑰的收件人能夠決定該實體是否是簽名者。

在本發明具體實施例中，數位簽名515被產生的方式為，使用簽名者的金鑰525，例如，中央伺服器(請參閱圖2)的金鑰、應用500、使用權限清單505及開發者識別資訊510當作數

五、發明說明 (16)

位簽名演算法 530 的輸入。結果是取決於內含於輸入中之資訊的數位簽名 515。

建立數位簽名 515 之後，將應用 500、使用權限清單 505、開發者識別資訊 510 及數位簽名 515 傳輸至無線裝置 520。然後，無線裝置可使用數位簽名以決定任何應用或相關資訊(即，使用權限清單及開發者識別資訊)是否被修改。此外，使用如上文所述的技術之一，如安全鑰，無線裝置也可擁有將這項資訊傳輸至無線裝置之簽名者身份方面的可信度。

圖 6 顯示用於解說根據本發明示範性具體實施例方法之用於散發應用之伺服器使用之步驟的流程圖。在本示範性具體實施例中，處理程序從接收一應用及一數位簽名開始(步驟 600)。數位簽名是與應用相關的資訊，以便可決定在接收到應用之前，應用是否已被修改。另外，最好可由第三方指派用於簽署數位簽名的金鑰，以便驗證在應用上簽名的實體或開發者是接收所指派金鑰的開發者。

接收到應用及數位簽名後，該數位簽名被評估以決定傳送該應用的開發者與簽署應用者是同一人(步驟 605)。如果第三方將建立數位簽名的金鑰指派給開發者，則第三方也會將用於評估數位簽名的金鑰指派給接收方，如指派給參考圖 2 所述的中央伺服器。

接著，無論是簽署及/或建立應用的實體，開發者的識別被儲存並且與該應用關聯(步驟 610)。儲存裝置可能是表格、資料庫或其他方式，以便之後如果需要決定開發者身份時可被擷取。在一項具體實施例中，開發者識別的儲存裝置係

五、發明說明 (17)

儲存在無線裝置中，而不是儲存在伺服器上。

然後，認證所接收應用，以決定其是否符合指定的準則(步驟615)。在一項具體實施例中，應用可被選寫以在指定平台上執行，如總公司位於美國加州聖地牙哥 QUALCOMM Incorporated公司開發之在無線裝置上使用的 BREW™ 平台。特定平台或裝置可具有特定需求，以使應用必須先符合特定需求才能在裝置上執行。例如，平台或裝置可能要求應用不可存取裝置中的特定記憶體位置，使裝置的完整性或位於記憶體中的其他應用不會受到影響。這些準則可被指定，並且應用可經過測試，以決定是否符合這些準則。最好這些準則係預先決定並且提供給開發者，以併入應用開發中。

認證之後，指派與適用於給定環境之應用關聯的使用權限(步驟620)。可以許多因數為基礎來指派使用權限，視實施本發明的環境而定。在一項具體實施例中，應用預定適用於無線裝置。例如，在本具體實施例中，指派的使用權限可取決於電信業者網路、無線裝置的需求、認證測試的結果及開發者、電信業者或其他測試環境。因此，使用權限清單的一項實例是指示應用通過認證測試，並且可在特定電信業者網路上執行。

然後，伺服器數位簽名應用、使用權限清單及開發者識別(步驟625)。在一項具體實施例中，使用安全鑰來執行簽名，以便可藉由接收這項數位簽名的資訊來決定伺服器的身份。這不需要簽署伺服器所接收的開發者簽名，也不需要將開發者簽名傳送至無線裝置。

五、發明說明 (18)

然後，可將應用、使用權限清單、開發者識別及步驟625建立的簽名傳送至無線裝置(步驟630)。

圖7顯示用於解說根據本發明示範性具體實施例方法之無線裝置執行應用時使用之步驟的流程圖。在本具體實施例中，無線裝置儲存用於評估與一應用關聯之使用權限的規則(步驟700)。熟知技藝人士應明白，雖然本發明說明規則/使用權限範例，但是有許多範例可用來將使用權限授予給適用於特定裝置或平台的應用，並且這些範例皆被視為屬於本發明的範疇。

然後，無線裝置接收應用、使用權限清單、開發者識別及數位簽名(步驟705)。在一項具體實施例中，無線裝置可評估所接收數位簽名，以決定簽名者的身份。數位簽名也可用來決定應用、使用權限清單或開發者識別及數位簽名在已簽署後是否有被修改。

然後，無線裝置接收一執行應用的要求(步驟710)。這項要求可能來自於想要執行程式之無線裝置的使用者。或者，可由無線裝置本身提出要求，或透過網路或直接連接至無線裝置之來自於傳輸至無線裝置的某種要求。

接收到要求之後，在執行應用之前，無線裝置先評估與應用關聯的數位簽名及使用權限清單(步驟720)。如所述，在一項具體實施例中，無線裝置可使用規則來評估使用權限清單。如果藉由評估數位簽名而決定應用、使用權限清單或開發者識別未被修改，則無線裝置使用所儲存規則來評估使用權限清單。如果未被修改，並且比對使用權限清單評估規

五、發明說明 (19)

則指示授予應用在無線裝置中執行的使用權限，則處理程序進行到在裝置上執行應用(步驟730)。

如果步驟720的評估指示應用、使用權限清單或開發者識別在簽署之後有被修改，或是指示拒絕應用在無線裝置上執行的權限，則不會執行應用(步驟725)。處理程序進行到從無線裝置移除應用(步驟750)。最好也從無線裝置移除使用權限清單及開發者識別。

步驟730之後，監視應用的執行過程，以決定其是否有執行非法或不適當的作業(步驟735)。無線裝置或無線裝置使用的平台可定義屬於非法或不適當作業的特定作業。這些作業可包括存取記憶體的限制區域，或其他程式或檔案使用的記憶體位置。此外，這些作業可涉及有害使用無線裝置的資源，因而不僅會影響無線裝置，而且還會影響無線裝置所連接之網路上的其他裝置。

如果嘗試此類的非法或不適當的作業，則會停止執行應用(步驟745)，並且從無線裝置移除(步驟750)，最好連同開發者識別與使用權限清單一起移除。如上文所述，或者，移除處理程序可涉及停用應用，藉此防止執行應用，並且將應用保存在無線裝置上。

如果於步驟735沒有執行非法、不適當或非期望的作業，則會允許繼續執行應用(步驟740)。

結論

使用機制進行認證、偵測修改、決定來源身份、指派使用權限及併入移除應用功能，藉由引用本文中說明及提出的

五、發明說明 (20)

所有技術，根據本發明的系統及方法增加安全且牢靠的應用散發及執行。系統及方法可實施幾個或所有這些機制。實施的機制愈多，則達成的安全度愈高。

在一項具體實施例中，開發者將應用傳送至伺服器。開發者可在應用上簽名以防止未經授權修改。伺服器檢查開發者身份，並且執行應用的認證測試。伺服器也將一使用權限指派給該應用，建立一使用權限清單。應用、使用權限清單、開發者識別經過伺服器的數位簽名，並且連同數位簽名一起傳送至無線裝置。在執行應用之前，無線裝置先檢查數位簽名以得知是否有修改，並且比對所儲存的規則檢查使用權限清單。在一項具體實施例中，每當嘗試在無線裝置上執行應用時，都會執行這些檢查。如果檢查結果指示應用已被修改或拒絕准許執行，則不會執行應用，並且從無線裝置移除該應用。另外，於執行期間，如果應用嘗試非法或不適當的作業，則會終止應用，然後從無線裝置移除該應用。

基於圖解及說明的目，前面已提出本發明實施的說明書。它不是預計詳細說明本發明，並且不使本發明限定於發表的確切形式。可按照上述的說明來修改及變化本發明，或從實施本發明獲得。例如，所說明的實施包括軟體，但是本發明的具體實施例可實施為軟硬體組合，或僅以硬體實施。本發明可用物件導向程式設計系統或非物件導向程式設計系統實施。此外，雖然所說明的本發明觀點係儲存在記憶體中，但是熟知技藝人士應明白，這些觀點也可儲存在其他類型的電腦可讀取媒體中，如次儲存裝置，像是硬碟機、軟碟片

五、發明說明 (21)

或 CD-ROM；來自於網際網路或其他傳播媒體的載波；或其他形式的 RAM 或 ROM。本發明係藉由隨附的申請專利範圍及其同等級所定義。

裝

訂

線

四、中文發明摘要(發明之名稱：無線環境中之安全應用散發及執行)

本發明揭示安全且牢靠的應用散發及執行，其方式是提供測試一應用之系統及方法，以確保符合與應用執行環境相關的預先決定準則。另外，藉由使用規則與權限清單、應用移除及如數位簽名之類的修改偵測技術，本發明提供機制以安全散發及執行經過測試或未經測試應用，其方式為決定該應用是否已被修改、決定該應用是否具有在一給定無線裝置環境中執行的權限，以及萬一希望移除該應用時移除該應用。

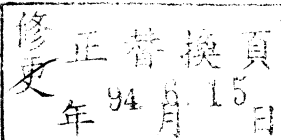
英文發明摘要(發明之名稱：SAFE APPLICATION DISTRIBUTION AND EXECUTION IN A WIRELESS ENVIRONMENT)

The present invention provides safe and secure application distribution and execution by providing systems and methods that test an application to ensure that it satisfies predetermined criteria associated with the environment in which it will execute. Furthermore, by using rules and permission lists, application removal, and a modification detection technique, such as digital signatures, the present invention provides mechanisms to safely distribute and execute tested, or untested, applications by determining whether the application has been modified, determining if it has permission to execute in a given wireless device environment, and removing the application should it be desirable to do so.

五、發明說明 (22)

主要元件符號說明

200	開發者
205	中央伺服器
210	認證伺服器
215	應用下載伺服器
220	無線網路
230	無線裝置
300	網路
302	中央伺服器
304	中央伺服器資料庫
306	伺服器
308	網路
310	載體網路
311	傳統舊式電話系統或網際網路
312	MSC
314	基地台
316	移除命令
322	移除命令來源
330	無線裝置
400	無線裝置
405	儲存器
410	應用程式介面
415	專用積體電路
420	本機資料庫
425	應用及使用權限清單
430	按鍵
435	規則
500	應用
505	使用權限清單
510	開發者識別資訊
515	數位簽名
520	無線裝置
525	簽名者的金鑰
530	數位簽名演算法



六、申請專利範圍

1. 一種散發及處理一應用之方法，該方法包括下列步驟：
接收該應用及識別資訊；
認證該應用符合一預先決定準則；
將一使用權限指派給該應用；
使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置；
決定於傳輸期間該應用是否有被修改；
在該裝置上儲存一規則；
使用該使用權限及該規則來決定是否可處理該應用；
以及
從該裝置移除該應用。
2. 如申請專利範圍第1項之方法，進一步包括下列步驟：
在傳輸該應用、該使用權限及該識別資訊至一裝置之後，使用一修改偵測技術，
起始在該裝置上執行該應用；
監視該應用之執行；以及
偵測該應用是否嘗試進行一不適當作業。
3. 如申請專利範圍第1項之方法，其中利用該使用權限與該規則決定是否可處理該應用之步驟包括拒絕准許在該裝置上處理該應用。
4. 如申請專利範圍第1項之方法，其中該識別資訊係由該裝置擷取。
5. 如申請專利範圍第1項之方法，進一步包括下列步驟：
在傳輸該應用、該使用權限及該識別資訊至一裝置之

六、申請專利範圍

- 後，使用一修改偵測技術，偵測該應用中之一修改。
6. 如申請專利範圍第1項之方法，進一步包括下列步驟：
- 在傳輸該應用、該使用權限及該識別資訊至一裝置之後，使用一修改偵測技術，偵測該使用權限之一修改。
7. 如申請專利範圍第1項之方法，其中該修改偵測技術使用一數位簽名。
8. 一種散發與處理一應用之方法，該方法包括下列步驟：
- 接收該應用及識別資訊；
- 認證該應用符合一預先決定準則；
- 將一使用權限指派給該應用；
- 將該應用、該使用權限及該識別資訊傳輸至一無線裝置；
- 在該裝置上儲存一規則；以及
- 使用該使用權限及該規則來決定是否可在該裝置上處理該應用。
9. 如申請專利範圍第8項之方法，進一步包括下列步驟：
- 在傳輸該應用、該使用權限及該識別資訊至該無線裝置之後，
- 起始在該裝置上執行該應用；
- 監視該應用之執行；
- 偵測該應用是否嘗試進行不一適當作業；以及
- 從該無線裝置移除該應用。
10. 如申請專利範圍第8項之方法，其中利用該使用權限與該規則決定是否可處理該應用之步驟，包括：

六、申請專利範圍

拒絕准許在該無線裝置上處理該應用；及

從該裝置移除該應用。

11. 如申請專利範圍第8項之方法，其中該識別資訊係由該無線裝置決定。

12. 如申請專利範圍第8項之方法，其中一修改偵測技術係用來傳輸該應用、該使用權限及該識別資訊。

13. 如申請專利範圍第12項之方法，其中該修改偵測技術使用一數位簽名。

14. 如申請專利範圍第12項之方法，進一步包括下列步驟：

在傳輸該應用、該使用權限及該識別資訊至該無線裝置之後，偵測是否有修改傳輸至該裝置的該應用；以及
從該裝置移除該應用。

15. 如申請專利範圍第12項之方法，進一步包括下列步驟：

在傳輸該應用、該使用權限及該識別資訊至該無線裝置之後，偵測是否有修改傳輸至該無線裝置的該使用權限；以及
從該裝置移除該應用。

從該裝置移除該應用。

16. 一種散發與處理一應用之方法，該方法包括下列步驟：

接收該應用及識別資訊；

將一使用權限指派給該應用；

使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置；

決定於傳輸期間該應用是否有被修改；

在該裝置上儲存一規則；

六、申請專利範圍

使用該使用權限及該規則來決定是否可處理該應用；
以及

從該裝置移除該應用。

17. 如申請專利範圍第16項之方法，進一步包括下列步驟：
在傳輸該應用、該使用權限及該識別資訊至該無線裝置之後，起始在該無線裝置上執行該應用；
監視該應用之執行；
偵測該應用是否嘗試進行不適當作業；以及
從該無線裝置移除該應用。
18. 如申請專利範圍第16項之方法，其中利用該使用權限與該規則決定是否可處理該應用之步驟，包括拒絕准許在該無線裝置上處理該應用。
19. 如申請專利範圍第16項之方法，其中該識別資訊係由該無線裝置決定。
20. 如申請專利範圍第16項之方法，其中一修改偵測技術係用來傳輸該應用、該使用權限及該識別資訊。
21. 如申請專利範圍第20項之方法，其中該修改偵測技術使用一數位簽名。
22. 如申請專利範圍第20項之方法，其中使用一修改偵測技術在傳輸該應用、該使用權限及該識別資訊之後，進一步包括偵測傳輸至該裝置該應用中之一修改。
23. 如申請專利範圍第20項之方法，其中使用一修改偵測技術在傳輸該應用、該使用權限及該識別資訊之後，進一步包括偵測傳輸至該裝置該使用權限中之一修改。

六、申請專利範圍

24. 一種用於在一無線裝置上散發與執行一應用之系統，該系統包括：

一中央伺服器，其被操作以接收該應用及開發者識別、指派一與該應用關聯的使用權限，以及將該應用資訊傳輸至該無線裝置；

一伺服器，其被操作以認證該應用符合一預先定義準則；以及

該無線裝置被操作，以接收該應用及該開發者識別，並且評估所指派的使用權限。

25. 如申請專利範圍第24項之系統，其中該中央伺服器進一步被操作，以使用一修改偵測技術將該應用傳輸至該無線裝置。

26. 如申請專利範圍第24項之系統，其中該中央伺服器進一步被操作，以使用一修改偵測技術將該使用權限傳輸至該無線裝置。

27. 如申請專利範圍第24項之系統，其中被操作以認證該應用的該伺服器是該中央伺服器。

28. 如申請專利範圍第24項之系統，其中該無線裝置被操作，以使用一儲存於該無線裝置中的規則來評估該指派的使用權限。

29. 一種用於在一無線裝置上散發與執行一應用之系統，該系統包括：

接收裝置，用於接收該應用及識別資訊；

指派裝置，用於將一使用權限指派給該應用；

六、申請專利範圍

傳輸裝置，用於使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至該裝置；

決定裝置，用於決定於傳輸期間該應用是否有被修改；

儲存裝置，用於在該裝置上儲存一規則；

決定裝置，用於使用該使用權限及該規則來決定是否可處理該應用；以及

移除裝置，用於從該裝置移除該應用。

30. 一種處理應用散發之方法，該方法包括下列步驟：

接收該應用及識別資訊；

認證該應用符合一預先決定準則；

將一使用權限指派給該應用；

使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置；以及

起始一要求，以從一裝置移除該應用。

31. 如申請專利範圍第30項之方法，其中在接收該應用與該識別資訊之後，進一步包括評估該已接收到的應用及識別資訊，以決定該應用之開發者身份。

32. 如申請專利範圍第30項之方法，其中該修改偵測技術使用一數位簽名。

33. 一種處理應用散發之方法，該方法包括下列步驟：

接收該應用及識別資訊；

將一使用權限指派給該應用；以及

使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置。

六、申請專利範圍

34. 如申請專利範圍第33項之方法，其中使用一修改偵測技術在傳輸該應用、該使用權限及該識別資訊至該裝置之後，進一步包括起始一要求以從一裝置移除該應用。
35. 如申請專利範圍第33項之方法，其中在接收該應用與識別資訊之後，進一步包括認證該應用程式符合一預先決定準則。
36. 如申請專利範圍第33項之方法，其中在接收該應用與識別資訊之後，進一步包括評估所該已接收到的應用與識別資訊，以決定該應用之開發者身份。
37. 如申請專利範圍第33項之方法，其中該修改偵測技術使用一數位簽名。
38. 一種應用散發系統，該系統包括：
 - 一中央伺服器，其被操作以接收該應用及識別資訊、指派一使用權限，以及使用一修改偵測技術傳輸該應用；以及
 - 一網路，其被連接到該中央伺服器以接收該應用。
39. 如申請專利範圍第38項之系統，其中該中央伺服器進一步被操作，以認證該應用符合一預先定義準則。
40. 一種應用散發系統，該系統包括：
 - 接收裝置，用於接收該應用及識別資訊；
 - 認證裝置，用於認證該應用符合一預先決定準則；
 - 指派裝置，用於將一使用權限指派給該應用；以及
 - 傳輸裝置，用於使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至該裝置。

六、申請專利範圍

41. 一種包含用於散發應用之電腦可執行指令之電腦可讀取媒體，包括下列步驟：
- 接收該應用及識別資訊；
 - 認證該應用符合一預先決定準則；
 - 將一使用權限指派給該應用；以及
 - 使用一修改偵測技術將該應用、該使用權限及該識別資訊傳輸至一裝置。
42. 一種用於在一無線裝置上執行一應用之方法，該方法包括下列步驟：
- 儲存一用於評估一使用權限的規則；
 - 使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；
 - 接收一用於在該無線裝置上執行該應用的要求；
 - 評估該所接收資訊以決定該所接收資訊是否有被修改；
 - 如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及
 - 如果授予該使用權限，則執行該應用。
43. 如申請專利範圍第42項之方法，其中該修改偵測技術使用一數位簽名。
44. 如申請專利範圍第42項之方法，其中在接收一要求以便在該無線裝置上執行該應用之後，進一步包括監視該應用的執行以決定是否有嘗試一不適當作業。
45. 如申請專利範圍第42項之方法，進一步包括：
- 若修改該資訊或者不准許該使用權限，移除該應用。

六、申請專利範圍

46. 一種在一無線裝置上執行一應用之方法，包括下列步驟：
- 儲存一用於評估一使用權限的規則；
 - 使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；
 - 接收一用於在該無線裝置上執行該應用的要求；
 - 評估所接收資訊以便決定是否修改所接收資訊；以及
 - 假使該資訊有被修改，則從該無線裝置移除該應用。
47. 如申請專利範圍第46項之方法，其中在評估所接收資訊以便決定是否修改所接收資訊之後，進一步包括下列步驟：
- 如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及
 - 如果授予該使用權限，則執行該應用。
48. 如申請專利範圍第46項之方法，其中該修改偵測技術使用一數位簽名。
49. 如申請專利範圍第47項之方法，其中在執行該應用之後，進一步包括監視該應用的執行以決定是否有嘗試一不適當作業。
50. 如申請專利範圍第49項之方法，進一步包括假使嘗試不適當作業，則從該無線裝置移除該應用的步驟。
51. 一種執行一應用之無線裝置，包括：
- 一輸入，用於接收一應用及一使用權限；
 - 一規則，其內含於儲存裝置中，用於評估該使用權限；以及

六、申請專利範圍

一金鑰，其內含於儲存裝置中，用於評估一數位簽名，其中該無線裝置被操作，以在評估該使用權限與該數位簽名後執行該應用。

52. 一種執行一應用之無線裝置，包括：

儲存裝置，用於儲存一用於評估一使用權限的規則；

接收裝置，用於使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；

接收裝置，用於接收一用於在該無線裝置上執行該應用的要求；

評估裝置，用於評估該所接收資訊以決定該所接收資訊是否有被修改；

評估裝置，用於如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及

執行裝置，用於如果授予該使用權限，則執行該應用。

53. 一種包含用於散發應用之電腦可執行指令之電腦可讀取媒體，包括下列步驟：

儲存一用於評估一使用權限的規則；

使用一修改偵測技術接收包含該應用、該使用權限及該識別資訊的資訊；

接收一用於在該無線裝置上執行該應用的要求；

評估該所接收資訊以決定該所接收資訊是否有被修改；

如果該所接收資訊未被修改，則評估與該應用相關的該使用權限；以及

如果授予該使用權限，則執行該應用。

第 091111721 號專利申請案
中文圖式替換本(94年11月)

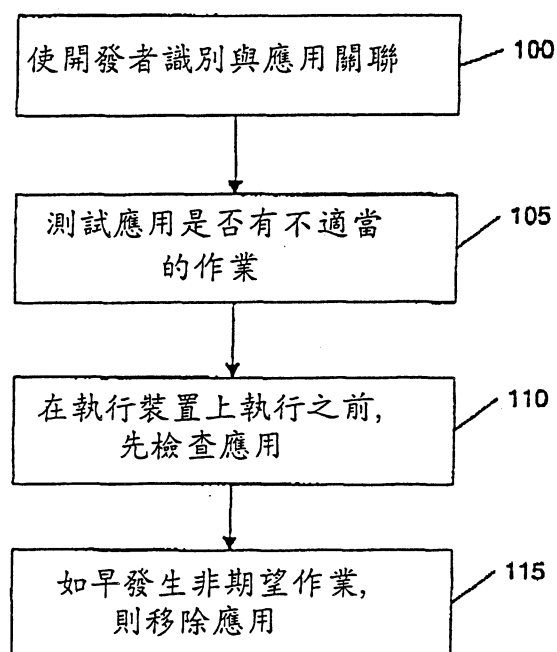


圖 1

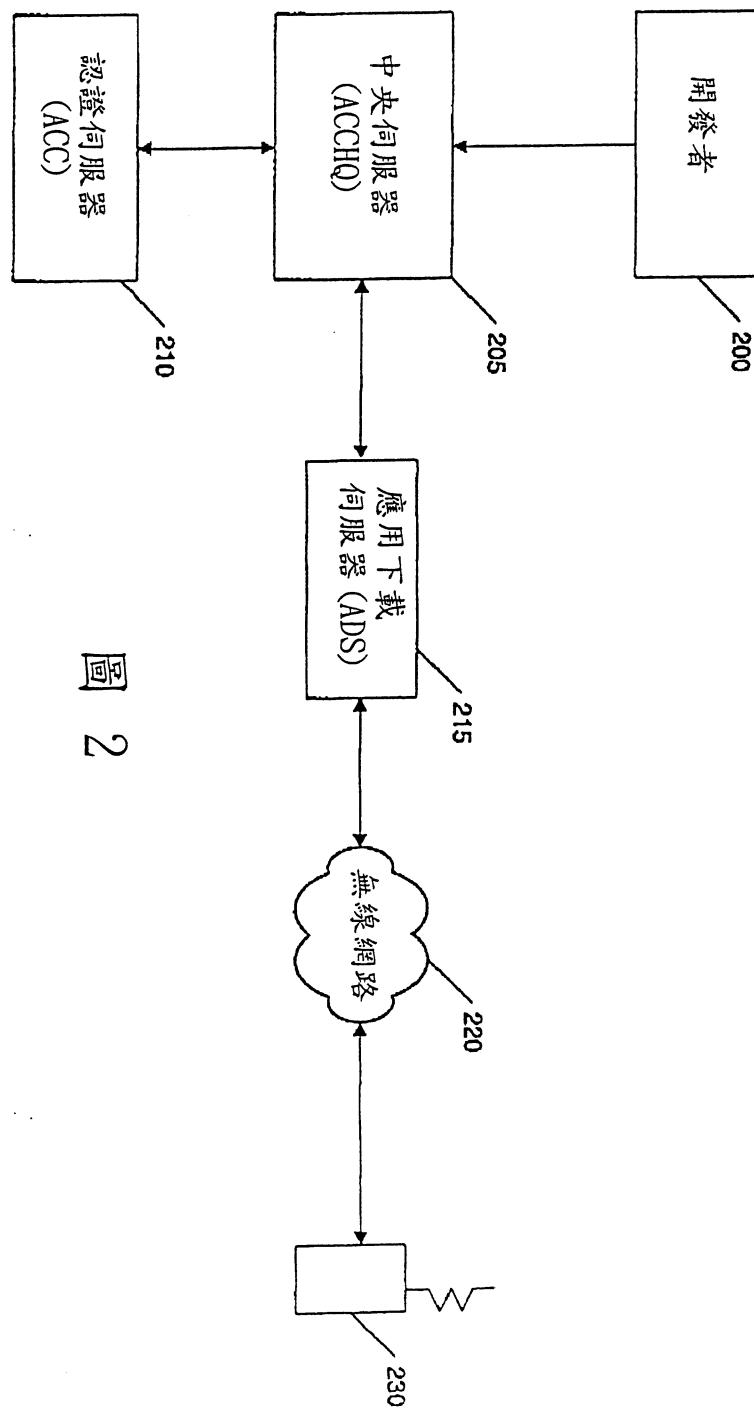


圖 2

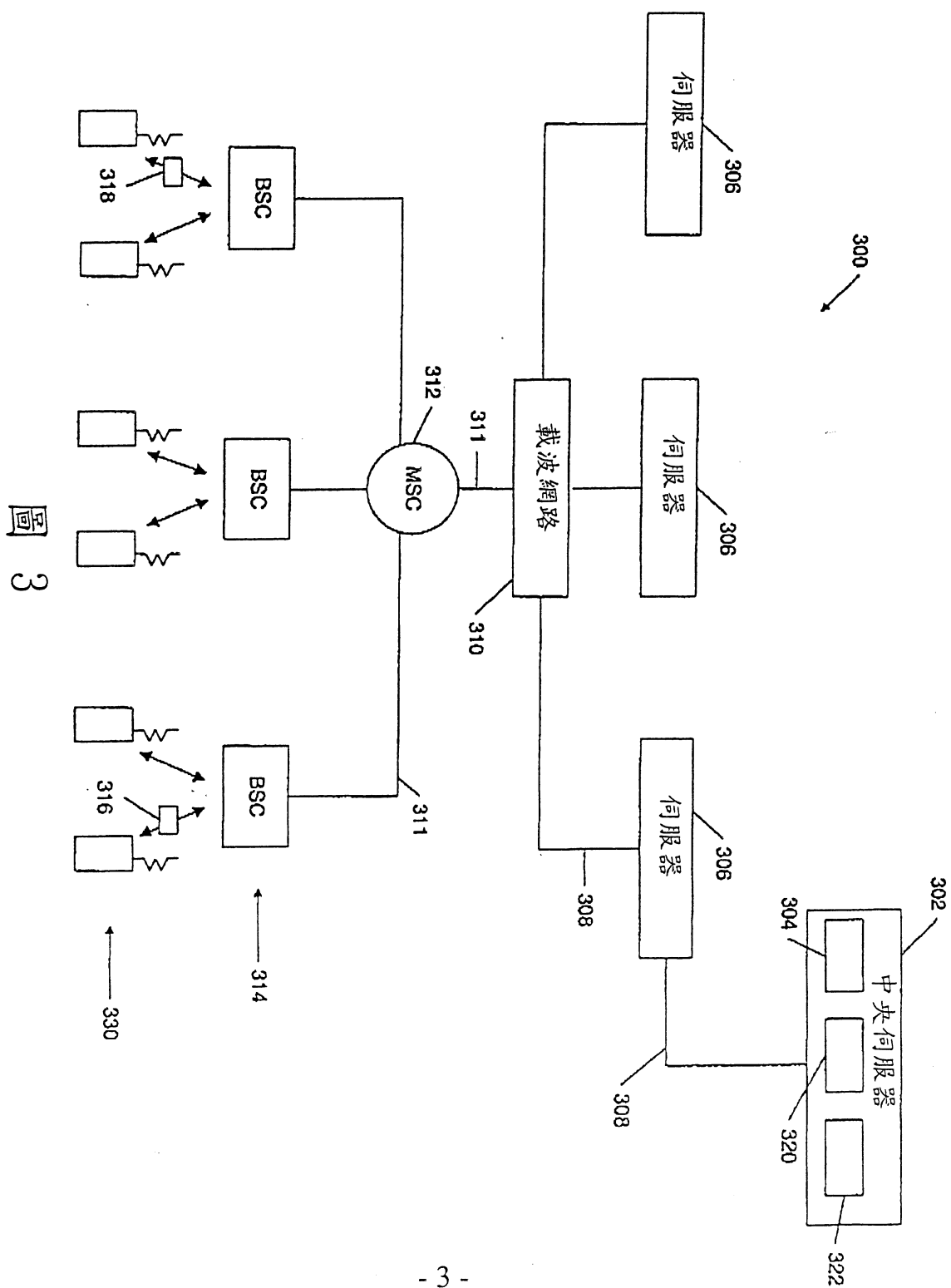


圖 3

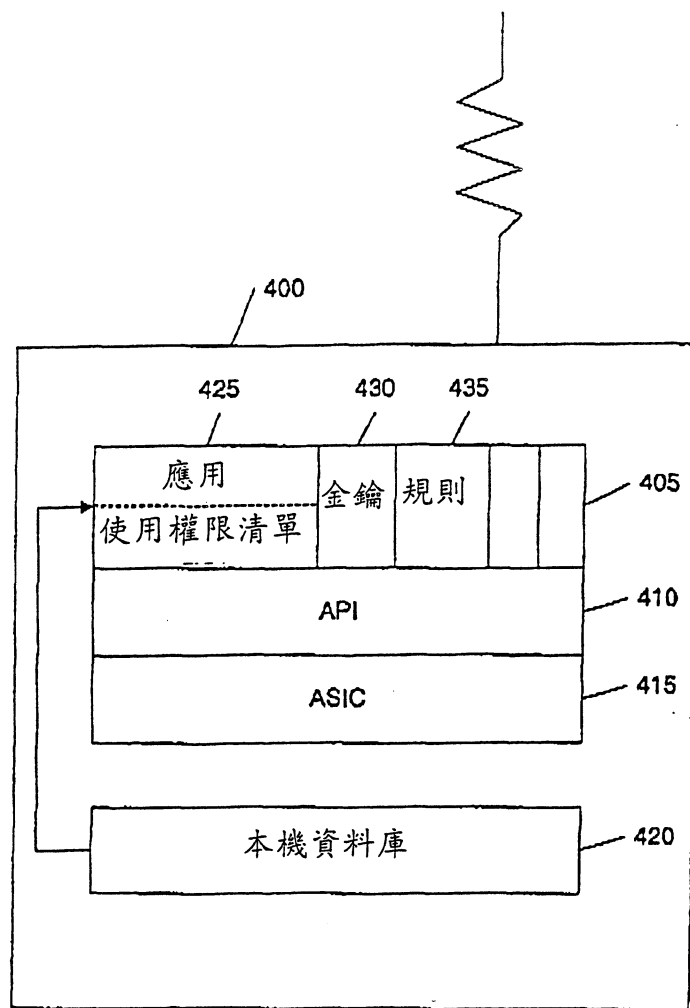


圖 4

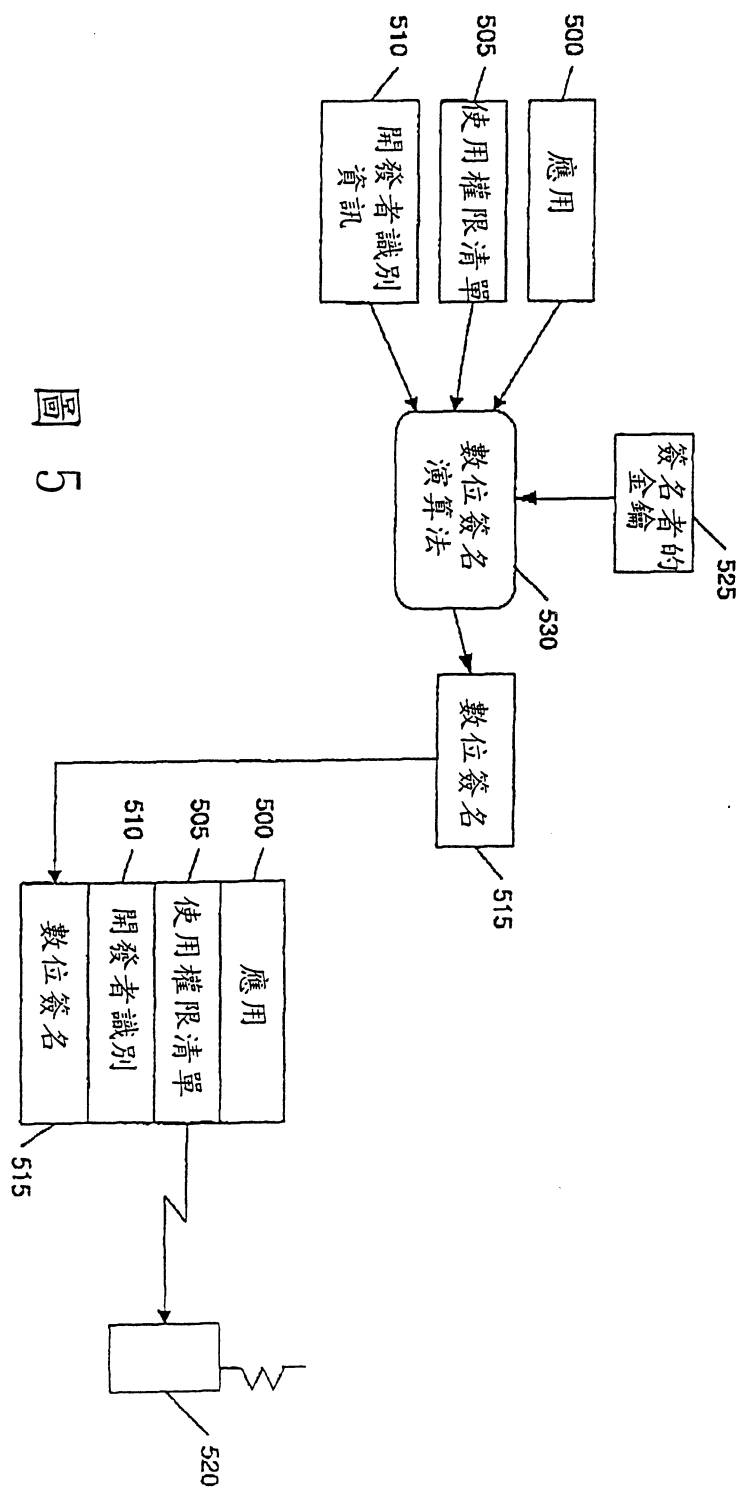


圖 5

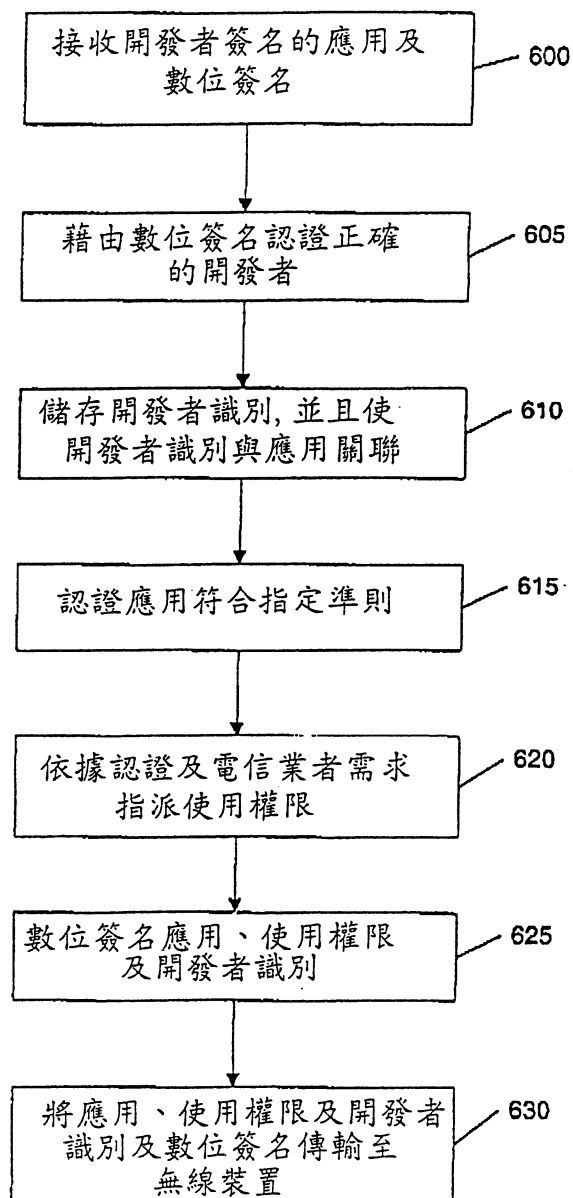


圖 6

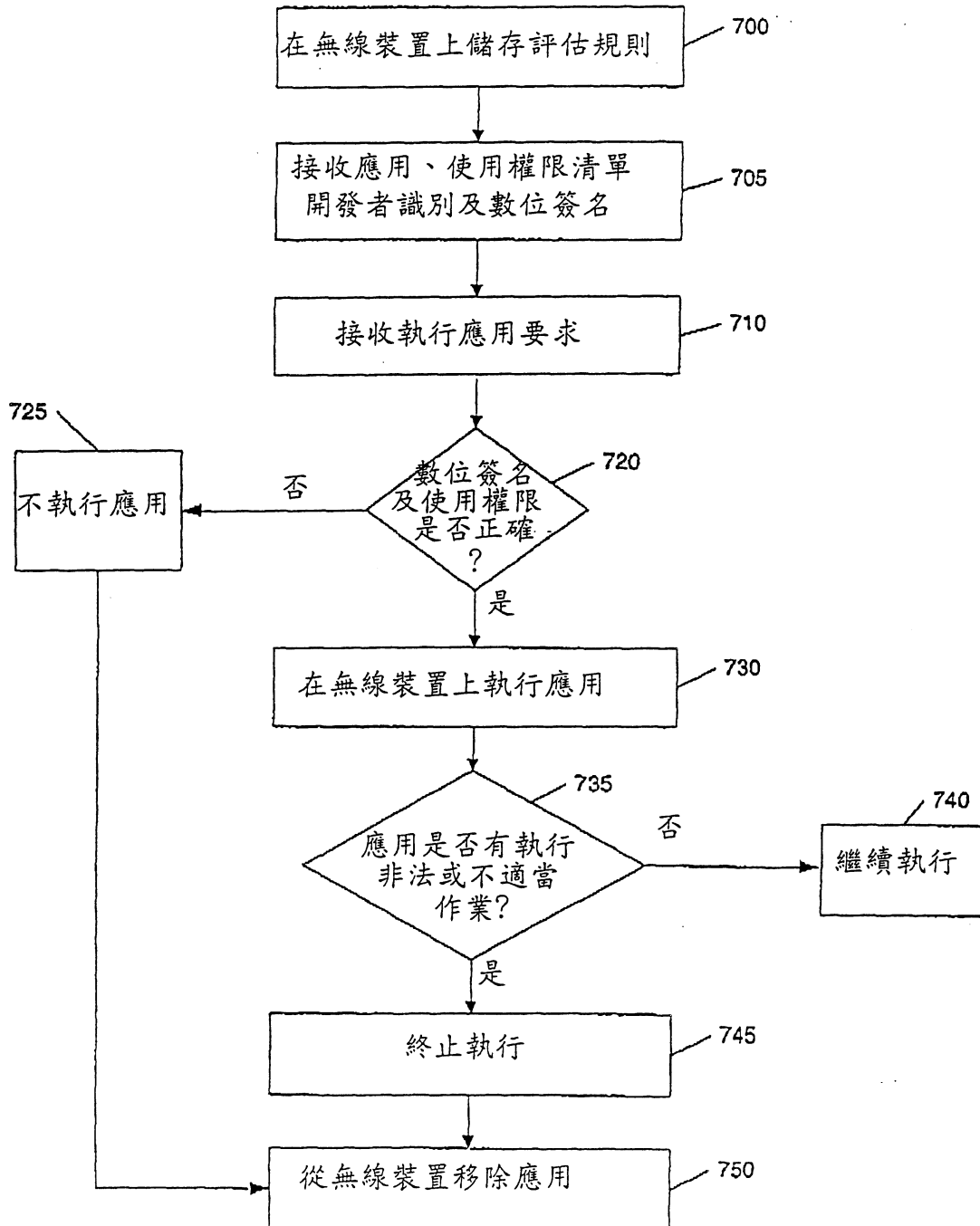


圖 7