(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201403377 A
(43)公開日： 中華民國 103 (2014) 年 01 月 16 日

(21)申請案號：102122766 (22)申請日： 中華民國 102 (2013) 年 06 月 26 日
(51)Int. Cl.： *G06F21/73 (2013.01)* *G06F21/60 (2013.01)*
(30)優先權：2012/06/26 美國 61/664,465
2013/06/25 美國 13/926,533
(71)申請人：歐樂岡科技公司 (列支敦斯登) OLOGN TECHNOLOGIES AG (LI)
列支敦斯登
(72)發明人：伊納貞克 瑟吉 IGNATCHENKO, SERGEY (CA)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：36 項 圖式數：3 共 28 頁

(54)名稱

用於裝置之應用程式特定識別之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR THE APPLICATION-SPECIFIC IDENTIFICATION OF DEVICES

(57)摘要

本文描述提供管理裝置之應用程式特定識別之一計算環境之系統、方法及設備。根據本發明之一設備可包括儲存識別符(ID)基本資料之一非揮發性儲存器及一處理器。該處理器可經組態以驗證正在該設備上執行之一應用程式之一憑證。該憑證可含有該應用程式之一程式碼簽章者之一程式碼簽章者 ID。該處理器可經進一步組態以接收該應用程式之唯一 ID 之一請求、自該程式碼簽章者 ID 及該 ID 基本資料產生該唯一 ID 且傳回該所產生的唯一 ID。

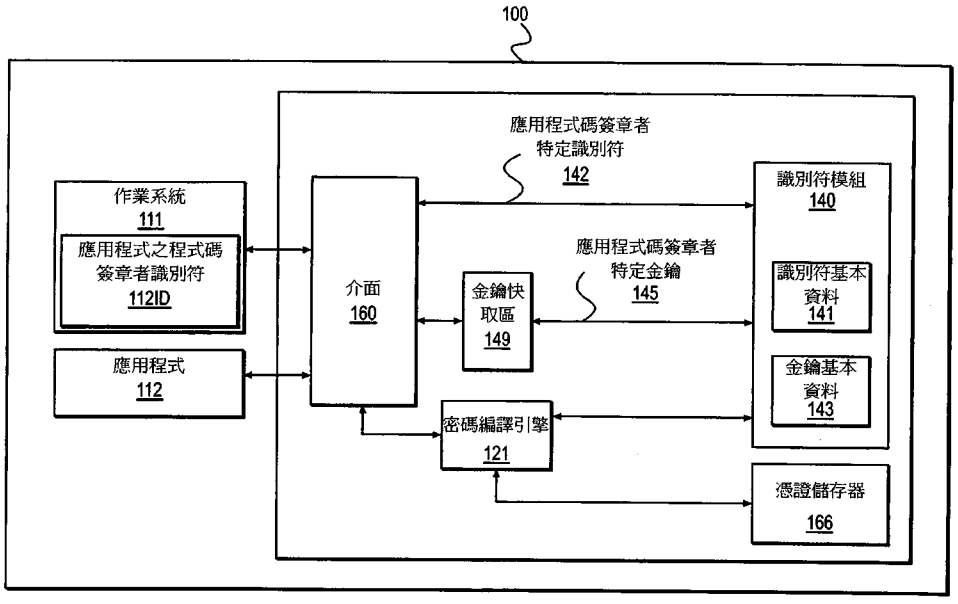

圖1

100：計算裝置
111：作業系統
112：應用程式
112ID：程式碼簽章者識別符
121：密碼編譯引擎
140：識別符模組
141：識別符基本資料
142：應用程式碼簽章者特定識別符
143：金鑰基本資料
145：應用程式碼簽章者特定金鑰對
149：金鑰快取區
160：介面
166：記憶體

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201403377 A
(43)公開日： 中華民國 103 (2014) 年 01 月 16 日

(21)申請案號：102122766 (22)申請日： 中華民國 102 (2013) 年 06 月 26 日
(51)Int. Cl.： *G06F21/73 (2013.01)* *G06F21/60 (2013.01)*
(30)優先權：2012/06/26 美國 61/664,465
2013/06/25 美國 13/926,533
(71)申請人：歐樂岡科技公司 (列支敦斯登) OLOGN TECHNOLOGIES AG (LI)
列支敦斯登
(72)發明人：伊納貞克 瑟吉 IGNATCHENKO, SERGEY (CA)
(74)代理人：陳長文
申請實體審查：無 申請專利範圍項數：36 項 圖式數：3 共 28 頁

(54)名稱

用於裝置之應用程式特定識別之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR THE APPLICATION-SPECIFIC IDENTIFICATION OF DEVICES

(57)摘要

本文描述提供管理裝置之應用程式特定識別之一計算環境之系統、方法及設備。根據本發明之一設備可包括儲存識別符(ID)基本資料之一非揮發性儲存器及一處理器。該處理器可經組態以驗證正在該設備上執行之一應用程式之一憑證。該憑證可含有該應用程式之一程式碼簽章者之一程式碼簽章者 ID。該處理器可經進一步組態以接收該應用程式之唯一 ID 之一請求、自該程式碼簽章者 ID 及該 ID 基本資料產生該唯一 ID 且傳回該所產生的唯一 ID。

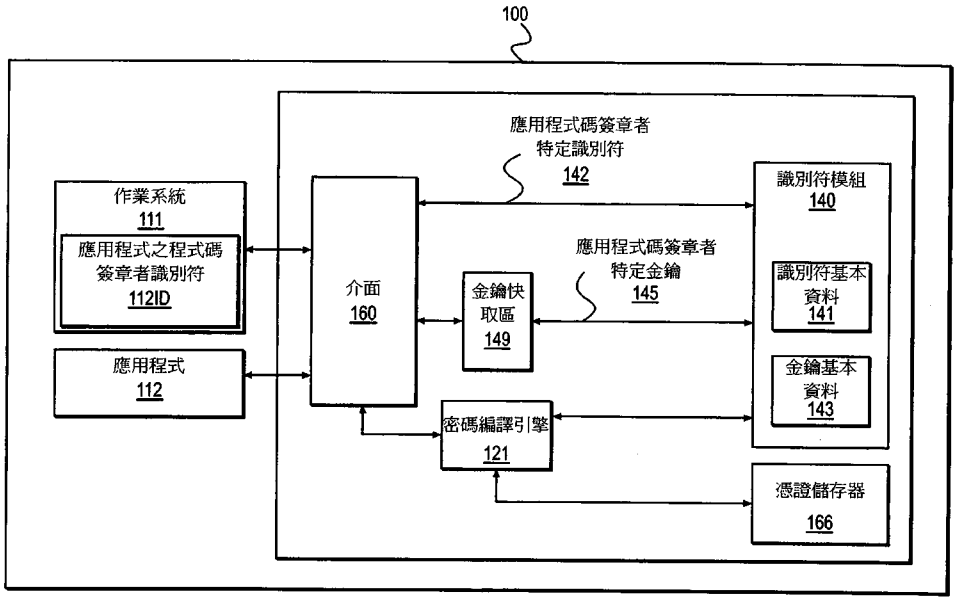

圖1

100：計算裝置
111：作業系統
112：應用程式
112ID：程式碼簽章者識別符
121：密碼編譯引擎
140：識別符模組
141：識別符基本資料
142：應用程式碼簽章者特定識別符
143：金鑰基本資料
145：應用程式碼簽章者特定金鑰對
149：金鑰快取區
160：介面
166：記憶體

發明摘要

※ 申請案號：102122766

※ 申請日：102.6.26

※IPC 分類：G06F 21/73 (2013.01)
G06F 21/60 (2013.01)

【發明名稱】

用於裝置之應用程式特定識別之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR THE APPLICATION-SPECIFIC IDENTIFICATION OF DEVICES

【中文】

本文描述提供管理裝置之應用程式特定識別之一計算環境之系統、方法及設備。根據本發明之一設備可包括儲存識別符(ID)基本資料之一非揮發性儲存器及一處理器。該處理器可經組態以驗證正在該設備上執行之一應用程式之一憑證。該憑證可含有該應用程式之一程式碼簽章者之一程式碼簽章者ID。該處理器可經進一步組態以接收該應用程式之唯一ID之一請求、自該程式碼簽章者ID及該ID基本資料產生該唯一ID且傳回該所產生的唯一ID。

【英文】

The systems, methods and apparatuses described herein provide a computing environment that manages application specific identification of devices. An apparatus according to the present disclosure may comprise a non-volatile storage storing identifier (ID) base data and a processor. The processor may be configured to validate a certificate of an application being executed on the apparatus. The certificate may contain a code signer ID for a code signer of the application. The processor may further be configured to receive a request for a unique ID of the application, generate the unique ID from the code signer ID and the ID base data and return the generated unique ID.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

100	計算裝置
111	作業系統
112	應用程式
112ID	程式碼簽章者識別符
121	密碼編譯引擎
140	識別符模組
141	識別符基本資料
142	應用程式碼簽章者特定識別符
143	金鑰基本資料
145	應用程式碼簽章者特定金鑰對
149	金鑰快取區
160	介面
166	記憶體

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】

用於裝置之應用程式特定識別之系統、方法及設備

SYSTEMS, METHODS AND APPARATUSES FOR THE APPLICATION-SPECIFIC IDENTIFICATION OF DEVICES

[相關申請案]

本申請案主張標題皆爲「Systems, Methods and Apparatuses for the Application-Specific Identification of Devices」之2012年6月26日申請之美國臨時申請案第61/664,465號及2013年6月25日申請之美國非臨時申請案第13/926,533號之優先權，該兩個申請案之內容係以引用方式全部併入本文。

【技術領域】

本文中描述之系統、方法及設備係關於對在電子裝置上執行之應用程式鑑認電子裝置並同時保護裝置及使用者隱私。

【先前技術】

多年來，諸如膝上型電腦、智慧型電話或平板電腦之計算裝置內之處理器使用全域識別符(ID)以對在裝置上執行之一或多個應用程式唯一地識別該裝置。有時候作業系統亦將具有此類型的全域ID。當容許第三方應用程式在一計算環境內執行時，此等應用程式由於多種合法原因而通常請求基礎硬體及/或作業系統之ID。例如，裝置特定ID可用以打擊欺詐、在官方發佈應用程式之准測試版之前鑑認對該等准測試版的存取且供電給特定行動廣告網路等等。

然而，給應用程式提供一全域識別符亦引起重要且熟習的隱私擔憂。例如，全域識別符有時候被用作諸如遊戲網路之行動網路之鑑

認機制。在此等情況中，若一攻擊者已獲取一使用者的裝置特定ID，則攻擊者能夠存取大量其他個人資料，包含關於一使用者連結的社交網站帳戶、使用者的電子郵件地址或使用者的行動電話號碼之資訊。隱私擔憂導致如Intel及Apple之此等公司停止使用全域ID。例如，在處理器之Pentium III系列之後由Intel開發之處理器不支援處理器序號(PSN)。作爲另一實例，Apple有限公司開始拒絕由第三方針對iOS平台開發之請求一唯一裝置識別符(UDID)之應用程式。

目前，不存在可藉以使於一計算裝置上執行之一應用程式僅存取其自身的應用程式特定ID及/或應用程式特定金鑰對之技術上及/或商業上可行的方法。目前可用的方法對所有應用程式提供單個全域ID，並不保護隱私不受惡意應用程式影響，或依賴於「以隱匿方式實現安全性(security by obscurity)」以加強隱私。

需要用於不容許應用程式存取全域ID或全域公開金鑰/私密金鑰對之裝置之安全、應用程式特定識別之系統、方法及設備。

【圖式簡單說明】

圖1係根據本發明之一例示性系統之一方塊圖。

圖2係根據本發明之請求且產生應用程式碼簽章者特定ID之例示性方法之一流程圖。

圖3A及圖3B係根據本發明之請求且產生應用程式碼簽章者特定金鑰(金鑰對)之例示性方法之流程圖。

【實施方式】

本文中結合下列描述及隨附圖式描述根據本發明之系統、設備及方法之某些闡釋性態樣。然而，此等態樣指示其中可採用本發明之原理且本發明旨在包含所有此等態樣及其等等效物之各種方式中的幾種方式。當結合圖式考慮時從下列【實施方式】可明白本發明之其他優點及新穎特徵。

在下列【實施方式】中，陳述數種特定細節以提供對本發明之一完整理解。在其他例項中，並未展示熟習結構、介面及程序以免不必要地混淆本發明。然而，一般技術者將明白，本文中揭示之特定細節無須用來實踐本發明且唯如申請專利範圍中敘述之外並不表示限制本發明之範疇。本說明書之部分皆不旨在被解釋爲實現否認本發明之全範疇之任何部分。雖然已描述本發明之某些實施例，但是此等實施例同樣不旨在限制本發明之全範疇。

本發明包括用於改良電子裝置之應用程式特定識別之系統、方法及設備。圖1展示根據本發明之一例示性計算裝置100之一方塊圖。一合適的計算裝置100可呈諸如一電腦、膝上型電腦、智慧型電話或平板電腦之一電子裝置之任何形式。

如圖1上展示，一計算裝置100可包括經組態以在該計算裝置100內之一中央處理單元(未展示)上執行之一或多個應用程式112或多段程式碼。在某些實施例中，該計算裝置100可具有一作業系統111，其中該一或多個應用程式112在該作業系統111之背景下執行。在其他實施例中，應用程式112可在無需一作業系統之情況下執行(例如，如關於標題爲「Secure Zone for Digital Communications」且申請於2012年4月13日之美國臨時專利申請案第61/623,861號描述)，該案之全部內容係以引用方式併入本文。

一計算裝置100可進一步包括一ID模組140。該ID模組140可包括(例如)能夠儲存至少一「ID基本資料」141及一「金鑰基本資料」143之記憶體。ID基本資料141及金鑰基本資料143二者皆可爲某個預定義大小之位元序列(其等可隨機產生)，該等位元係專用於各ID模組140。

如下文將進一步詳細論述，該ID模組140亦可經組態以提供應用程式碼簽章者特定ID 142及/或應用程式碼簽章者特定金鑰對145。此

等應用程式碼簽章者特定ID 142及金鑰對145可能係關於ID基本資料141或金鑰基本資料143使得i)其可明確地確定應用程式碼簽章者特定ID 142及應用程式碼簽章者特定金鑰對145分別自該ID基本資料141及該金鑰基本資料143導出，但是ii)不可能自該應用程式特定ID 142或該應用程式特定金鑰對145導出相關ID基本資料141或金鑰基本資料143。該ID模組140可進一步包括硬體及/或軟體(未展示)以完成本文中描述的功能性。

術語「程式碼簽章者(code signer)」指代數位地簽章應用程式112之實體。雖然開發(例如，編寫)程式碼之實體通常係數位地簽章程式碼之實體，但是情況並非總是如此且並非本發明之要求。應瞭解單個程式碼簽章者可簽章多個應用程式且各應用程式可具有不同版本。

一ID基本資料141可用於對一應用程式碼簽章者特定唯一地識別該計算裝置100之一程序中，且在某些實施例中可儲存在該ID模組140之非揮發性記憶體中。例如且無限制，該ID基本資料141可在製造時被硬編碼在該計算裝置100中，或於首次開啓計算裝置100電源產生時。在此等實施例中，該ID基本資料141不能變化。可期望確保不能自該計算裝置100提取或以其他方式危及該ID基本資料141。例如，該ID模組140內之記憶體可爲抗破壞記憶體及/或防篡改(tamper-evident)記憶體。亦可期望確保該作業系統111及/或在該計算裝置100上執行之任何應用程式112並不直接存取該ID基本資料141且不被容許讀取該ID基本資料141。

類似地，可於產生專用於藉由一特定程式碼簽章者簽章之在一裝置特定100上執行之應用程式112之加密金鑰之程序中使用金鑰基本資料143。此等唯一金鑰可用以(例如)傳遞資料至該裝置100，其中不能由任何其他裝置存取該資料，且甚至不能由藉由任何其他應用程式之程式碼簽章者簽章之在該裝置100上執行之一任務或應用程式存取

該資料。如圖1中所示且如下文更詳細描述，可在該ID模組140中之一非揮發性記憶體內產生且儲存一金鑰基本資料143。正如該ID基本資料141，可期望確保不能自該計算裝置100提取或以其他方式危及金鑰基本資料143，且確保該作業系統111及/或在該計算裝置100上執行之任何應用程式112並不直接存取該金鑰基本資料143。可(但非必須)於產生該ID基本資料141的同時產生該金鑰基本資料143。然而，一般而言，該ID基本資料141及該金鑰基本資料143二者皆可使用相同安全級別(例如，使用相同的品質隨機數產生器且具有相同數目個位元)而產生，且應使用相同的安全級別加以儲存且維持。

如下文將進一步詳細論述，當一應用程式112請求存取計算裝置的ID、存取計算裝置的公開金鑰或使用與該計算裝置100相關聯之一私密金鑰執行一操作時，該ID模組140可傳回一應用程式碼簽章者特定ID 142、一應用程式碼簽章者特定公開金鑰145PUB，或可使用一應用程式碼簽章者特定私密金鑰145PRIV。在某些實施例中，該計算裝置100可經組態以要求各應用程式112請求藉由應用程式的開發者或一程式碼簽章實體以鑑認應用程式之一方式數位地簽章一應用程式碼簽章者特定ID 142或一應用程式碼簽章者特定金鑰對145。若容許一些應用程式112在該計算裝置100內執行而不被簽章，則其等無法被容許請求一應用程式特定ID或金鑰對。

數位憑證驗證係許多作業系統之一標準特徵且可以各種方式加以實施。例如，該計算裝置100可檢查具備相關應用程式112之數位簽章及程式碼簽章者的數位憑證的有效性。如下文將更詳細描述，此等程式碼簽章者憑證通常包含用於識別程式碼簽章者之一機制。例如，若使用一X.509憑證，則通常在憑證內含有簽章者之一「辨別名稱」(distinguished name (DN))及「一般名稱」(common name (CN))。爲本發明之目的，該等或任何其他類似欄位(單獨或組合)可被用作一程式

碼簽章者ID 112ID。

程式碼簽章者憑證可藉由一或多個憑證機構(CA)簽章。這係用於保證一數位憑證之真實性之一般方法。在某些實施例中，該計算裝置100可包括用於儲存可用以執行一典型的公開金鑰基礎設施簽章驗證之一或多個CA根憑證之記憶體166。例如依據ITU-T-X.509標準發佈之一憑證將包含來自一CA之一數位簽章(或來自藉由一CA簽章之形成潛在任意長度之一PKI或似PKI憑證鏈之另一實體之一憑證)。

在某些實施例中，該計算裝置100可進一步包括可用於支援程式碼簽章者憑證驗證之一或多個密碼編譯引擎121等等。此等密碼編譯引擎121可經組態以實施一或多個密碼編譯演算法，諸如不對稱密碼演算法(Rivest-Shamir-Adleman(RSA))演算法或橢圓曲線密碼編譯學(ECC)或任何其他現有或未來開發的演算法。該計算裝置100亦可包括提供密碼編譯程序支援之一隨機數產生器(未展示)。

如下文將進一步詳細論述，在其中該ID模組140用以提供應用程式碼簽章者特定金鑰對145之實施例中，該計算裝置100可包含一選用金鑰快取區149。該金鑰快取區149可用以快取且滿足來自一應用程式112之金鑰請求。若使用來自金鑰快取區之一金鑰，則無須自該ID模組140請求一金鑰。

圖2、圖3A及圖3B展示根據本發明之例示性方法，藉由該等方法可分別請求、產生且傳回應用程式碼簽章者特定ID 142及應用程式碼簽章者特定金鑰對145至一應用程式112。

如圖2上所示，在步驟205處，可載入一應用程式112且驗證其憑證。例如，可載入該應用程式且可藉由該作業系統111驗證其憑證。在步驟210處，一應用程式112可發佈對一應用程式碼簽章者特定ID 142之一請求。可將該請求發佈至一介面160(或透過該介面160發佈該請求)。該介面160可爲任何合適的介面，包含(但不限於)硬體(例如，

一匯流排及/或處理邏輯)與軟體之一組合。

在步驟220處，可將應用程式之程式碼簽章者ID 112ID加至該請求，且可將該請求轉發至該ID模組140。若該應用程式112不具有一相關聯之程式碼簽章者ID 112ID，則對應用程式碼簽章者特定ID 142之此請求可失效。

在步驟230處，當接收到該請求時，該ID模組140可藉由組合該程式碼簽章者ID 112ID與該ID基本資料141且自此組合計算一單向雜湊函數來產生一應用程式碼簽章者特定ID 142。這確保該應用程式特定ID 142係一隨機位元序列。在一例示性實施例中，這可藉由以下各者來完成：採用程式碼簽章者ID 112ID作爲一字串、附加十六進位表示的ID基本資料141至該字串及計算所得字串之SHA-1雜湊值。應瞭解，獲得一應用程式碼簽章者特定ID 142之此特定方式僅僅係例示性且不旨在限制本發明之範疇。一般技術者將已知存在具有類似性質之數種其他組合。

在步驟240處，可將該應用程式碼簽章者特定ID 142傳回至請求應用程式112以供該應用程式使用。

本文中描述之系統經組態使得若發佈程式碼簽章者憑證給應用程式開發者，則各應用程式開發者將僅僅存取其自身的應用程式碼簽章者特定ID 142且將不能存取該ID基本資料141或任何其他應用程式開發者之ID。因此，一應用程式特定開發者將不能交叉分析其ID與來自其他應用程式開發者之ID。這可緩解與存在一全域ID有關的某些隱私擔憂，並同時仍供應用程式開發者之合法目的及需要使用。例如，該應用程式碼簽章者特定ID 142可用以限制由一特定計算裝置100產生之電子郵件帳戶、社交網站帳戶、遊戲網路帳戶等等之數目。

本發明之方法及系統可用以確保般僅藉由特定程式碼簽章者簽章之應用程式(程式碼簽章者指定的應用程式)才能存取安全資訊，

即，防止非被指定接收該資訊之裝置進行存取(或「竊取」)且亦防止其他程式碼簽章者簽章之任務或應用程式(非程式碼簽章者指定的任務或應用程式)進行存取(或「竊取」)，即使彼等任務或應用程式係在被指定接收該資訊之裝置上執行。例如，一遠端裝置(例如，一伺服器、電腦或類似或相似於該計算裝置100之遠端裝置)可發送被指定由藉由一特定程式碼簽章者開發之一應用程式112(該應用程式112在該計算裝置100上執行)接收及/或使用之一或多個訊息。可使用對應於與簽章該應用程式112之特定程式碼簽章者相關聯之應用程式碼簽章者特定私密金鑰之公開金鑰來加密該一或多個訊息。該計算裝置100上之被指定接收該一或多個訊息之應用程式112可使用該應用程式碼簽章者特定私密金鑰以解密該訊息。以此方式，可防止非該等訊息指定之其他程式碼簽章者及/或裝置之應用程式在該等訊息上進行存取(或「竊取」)。

在許多情況中，此等類型的操作將要求存在使裝置ID與公開金鑰相關聯之一外部資料庫。若各裝置僅僅具有一公開金鑰/私密金鑰對(即，該金鑰基本資料143)，則儘管使用一應用程式碼簽章者特定ID 142作爲一裝置ID，裝置公開金鑰亦仍爲各裝置獨有且將有效地用作一全域ID。若可透過唯一的公開金鑰識別裝置，則因此仍將存在與全域ID相關聯之所有隱私擔憂。

因此，在某些實施例中，可期望亦提供應用程式碼簽章者特定金鑰對145。圖3A展示可根據本發明憑藉其請求、產生且傳回一應用程式碼簽章者特定金鑰對145至一應用程式112之例示性方法。爲本發明之目的，假定已載入該應用程式且驗證其憑證。若這並未發生，則可在進行圖3A之方法之前執行類似於圖2中之步驟205之一步驟。

在步驟310處，一應用程式112可請求一密碼編譯操作。例如，該應用程式112可請求其公開金鑰，或可請求使用其私密金鑰加密或解

密一訊息。

在步驟320處，可將應用程式之程式碼簽章者ID 112ID加至該請求，且可將該請求轉發至該ID模組140。若可使用不同的密碼編譯演算法，則該請求亦可包含應使用之特定密碼編譯演算法之一識別。若該應用程式112不具有相關聯之程式碼簽章者ID 112ID，則此請求可失效。

在步驟330處，該ID模組140可產生一中間簽章者應用程式碼簽章者特定金鑰。在一例示性實施例中，可藉由以下各者產生此中間金鑰：採用該程式碼簽章者ID 112ID、組合該程式碼簽章者ID 112ID與該金鑰基本資料143、視需要添加一「密碼編譯salt值」，且接著計算所得組合之單向雜湊值。正如上文描述之應用程式碼簽章者特定ID，該中間金鑰係一隨機位元序列。

然而，不同於ID，在密碼編譯學中，已知某些位元序列取決於所使用的密碼編譯演算法提供較弱或較強的加密金鑰。對於任何給定的中間金鑰，存在其可能係正在使用的特定密碼編譯演算法之一「弱」金鑰之一可能性。術語「弱金鑰」大體上係用以意謂不適用於正在使用的特定密碼編譯演算法之任何金鑰。例如，若正在使用RSA演算法，則爲本發明之目的可將並未表示兩個質數之一「中間金鑰」視爲一「弱金鑰」。

在步驟340處，爲正在使用的加密演算法之目的，可篩選將爲弱的中間金鑰。具體如何完成此篩選程序可取決於正在使用的特定密碼編譯演算法。例如，對於DES演算法，存在16個目前被視爲「弱」及「半弱」金鑰之一清單；對於RSA演算法，並非一對質數之任何金鑰可被視爲「弱」。應注意，有些密碼編譯演算法不存在目前已知的弱金鑰且步驟340可基於目前密碼編譯知識而總是導致「肯定」回答。若判定對於使用中的密碼編譯演算法而言中間應用程式碼簽章者特定

金鑰爲弱(其經預定義或於步驟320中之請求中識別)，則該ID模組140可使用一不同的「密碼編譯salt值」重複步驟330，以產生中間應用程式碼簽章者特定金鑰。一旦中間金鑰足夠強以通過步驟340，在步驟350處其立即可變爲一應用程式碼簽章者特定金鑰145且可傳回至應用程式112。

在一些實施例中，可用在各反覆中使用的該金鑰基本資料143之一不同部分來取代(或增補)密碼編譯salt值。在此等實施例中，金鑰基本資料143應長於產生預定義加密演算法之金鑰所需最小長度。

可以一般技術者已知或在未來開發之任何合適的方式完成如何在每次執行步驟330時產生(或改變)一密碼編譯salt值。例如，密碼編譯salt值可爲在每次執行步驟330時遞增之一整數，或密碼編譯salt值可爲例如依據程式碼簽章者ID 112ID起始之一僞隨機數。

在一些實施例中，可使用例如依據程式碼簽章者ID 112ID起始之某種密碼編譯學上的安全僞隨機產生器(例如，虛擬亂數產生器(Blum-Blum-Shub產生器))作爲中間金鑰之來源，而非產生一密碼編譯salt值、將其附加至程式碼簽章者ID 112ID且使用雜湊值以產生一中間金鑰。

一般技術者將瞭解，在其中該應用程式碼簽章者特定金鑰145實際上係一不對稱金鑰對之實施例中，可能較佳的是，不容許應用程式112接收該私密金鑰145PRIV。若一應用程式112需要使用該私密金鑰145PRIV，則反而可將該私密金鑰145PRIV轉發至該密碼編譯引擎121，該密碼編譯引擎121可將所得密文傳回至該應用程式112而不揭露該私密金鑰145PRIV。

在本發明中，應用程式碼簽章者特定金鑰係確定性的。換言之，無關於是否使用一密碼編譯salt值、該金鑰基本資料143之一部分或一僞隨機產生器，且無關於所產生的金鑰145實際上是否係一不對

稱金鑰對，每當一應用程式112請求使用其私密金鑰時，應傳回相同的特定簽章者金鑰145。然而，獲得相同金鑰之程序可在不同實施例不斷變化。

在一實施例中，無須該ID模組140實際上將該應用程式碼簽章者特定金鑰145儲存在記憶體中。每當一應用程式112請求存取其金鑰145時可產生該應用程式碼簽章者特定金鑰145。這可改良系統之整體安全性及/或減小儲存需要。

然而，將瞭解取決於應用程式112之本質，可頻繁地重複此程序，這可降級整體系統效能。例如，產生一中間應用程式特定金鑰145、測試其密碼編譯強度及在發現一合適金鑰之前一直重複之步驟330至350(上文關於圖3描述)可能需要大量時間。因此，在一些實施例中，該計算裝置100可包括一金鑰快取區149。此金鑰快取區149係縮短滿足應用程式請求所需時間之一最佳特徵。

圖3B展示在併有一金鑰快取區149之一實施例中之一例示性方法，藉由該方法可請求、產生且傳回一應用程式特定金鑰對145至一應用程式112。唯此方法包含一額外步驟325之外，在步驟325中，在將對一應用程式特定金鑰之請求發送至該ID模組140之前，檢查該金鑰快取區149以判定對應於該請求應用程式112之一應用程式特定金鑰對145是否已儲存在該金鑰快取區149中，此方法類似於圖3A中描述之方法。若爲肯定，則無須重複步驟330及340，且該方法進行至步驟350，藉此將對應於該請求應用程式112之應用程式特定金鑰傳回至該應用程式。此外，在步驟360處，若私密金鑰145仍未儲存在該金鑰快取區149中，則將該私密金鑰145儲存在該金鑰快取區中。應注意，雖然在圖3B中圖解說明之實施例中，操作順序可彼此不同，但是在方法結束時傳回之金鑰仍保持確定性且取決於該金鑰基本資料143及該程式碼簽章者ID 112ID。

取決於整體系統需要，可使用多種密碼編譯演算法。爲應用程式碼簽章者特定金鑰145產生之目的，可期望選取一隨機位元序列被視爲一弱金鑰之概率較低之密碼編譯演算法。因此，將瞭解ECC可偏向於(例如)RSA。

雖然已關於一應用程式碼簽章者特定ID及應用程式碼簽章者特定金鑰對描述前述系統及方法，但是亦在本發明之範疇內產生且使用一應用程式特定獨有之一ID及/或金鑰對，可被稱爲(例如)一應用程式特定ID及一應用程式特定金鑰對。因此，可使用一應用程式特定ID以由相同開發者或程式碼簽章者唯一地識別不同的應用程式，且來自一特定程式碼簽章者之一特定應用程式可獨佔使用一應用程式特定金鑰對。進一步言之，亦在本發明之範疇內產生且使用一應用程式版本特定ID及/或一應用程式版本特定金鑰對。可使用一應用程式版本特定ID及金鑰對以唯一地識別來自一特定開發者或程式碼簽章者之一應用程式之一特定版本。在此等替代性實施例中，系統及方法反而可酌情地使用一應用程式ID或一應用程式版本ID，而非一程式碼簽章者ID 112ID。

注意在本文中描述之系統及方法中特定地使用加密僅僅係一可能的實施例。取決於整體系統約束及各種設備之能力，可用不對稱加密來替代對稱加密，且反之亦然。使用對稱金鑰或公開金鑰/私密金鑰密碼編譯學之特定組合以實施根據本發明之一系統事關藉由諸如可用以執行加密/解密之處理能力及完成加密/解密之速度的重要性之問題掌控之實施方案選取。亦應注意，亦可使用圖3A及圖3B中描述之方法以提供對稱金鑰來代替不對稱金鑰，或除不對稱金鑰之外提供對稱金鑰。

亦應注意，無論本發明內何時提及使用一不對稱金鑰(即，一公開金鑰或私密金鑰)加密一定的內容，其皆可實施爲使用不對稱金鑰

進行直接加密或替代地藉由產生一臨時安全密碼編譯的對稱金鑰、使用此臨時對稱金鑰加密該內容及使用一不對稱金鑰加密該臨時對稱金鑰而實施。接著，被加密的內容將包含使用該臨時對稱金鑰加密之內容以及使用該不對稱金鑰加密之臨時對稱金鑰二者。這係在密碼編譯學中在(例如)由於系統資源有限而無法期望使用不對稱加密來加密大量資料時用於最佳化目的之一標準技術(應瞭解，不對稱加密一般較慢且比對稱加密需要更多資源)。

亦應瞭解，可在安全計算區內實施本文中揭示之實施例。若作業系統足夠安全，則可透過作業系統自身來實施此一安全區，或可使用一基於硬體之安全區來實施此一安全區。一例示性基於硬體之安全區係在標題爲「Secure Zone for Digital Communications」且申請於2012年4月13日之美國臨時專利申請案第61/623,861號(該案之全部內容係以引用方式併入本文)中加以描述。

亦應瞭解，可使用支援程式碼簽章之任何作業系統實施本文中描述之實施例。一種此例示性作業系統係Apple有限公司開發之iOS作業系統。

雖然已圖解說明且描述本發明之特定實施例及應用，但是應瞭解本發明不限於本文中揭示之精確組態及組件。本文中使用的術語、描述及圖式係僅僅藉由圖解加以陳述且不意謂限制性。在不脫離本發明之精神及範疇之情況下，可對本文中揭示之本發明之設備、方法及系統之配置、操作及細節作出熟習此項技術者明白的各種修改、變化及變動。藉由非限制實例，將瞭解本文中包含的方塊圖旨在展示各設備及系統之組件之一選定子組，且各經描寫的設備及系統可包含該等圖式上未展示之其他組件。此外，熟習此項技術者將辨識，在無損於本文中描述之實施例之範疇或效能之情況下，可省略或重新排序本文中描述之某些步驟及功能性。

結合本文中揭示之實施例描述之各種闡釋性邏輯塊、模組、電路可實施爲電子硬體、電腦軟體或該二者之組合。爲圖解說明硬體與軟體之此可互換性，上文已在其等功能性方面大體上描述各種闡釋性組件、方塊、模組、電路及步驟。此功能性是否被實施爲硬體或軟體取決於特定應用程式及強加於整體系統之設計約束。對於各特定應用程式可以不同方式實施所描述的功能性--諸如藉由使用微處理器、微控制器、場可程式化閘陣列(FPGA)、特定應用積體電路(ASIC)及/或晶片上系統(SoC)之任何組合—但是此等實施方案決定不應被解譯爲導致背離本發明之範疇。

結合本文中揭示之實施例描述之一方法或演算法之步驟可直接具體實施於硬體、藉由一處理器執行之一軟體模組或該二者之一組合中。一軟體模組可駐留在RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、一可抽換式磁碟、一CD-ROM或此項技術者已知的任何其他形式的儲存媒體中。

本文中揭示之方法包括用於達成所述方法之一或多個步驟或動作。在不背離本發明之範疇之情況下，該等方法步驟及/或動作可彼此互換。換言之，除非實施例之適當操作需要一特定順序的步驟或動作，否則在不背離本發明之範疇之情況下可修改特定步驟及/或動作之順序及/或使用。

【符號說明】

100	計算裝置
111	作業系統
112	應用程式
112ID	程式碼簽章者識別符
121	密碼編譯引擎
140	識別符模組

141 識別符基本資料

142 應用程式碼簽章者特定識別符

143 金鑰基本資料

145 應用程式碼簽章者特定金鑰對

149 金鑰快取區

160 介面

166 記憶體

205 步驟

210 步驟

220 步驟

230 步驟

240 步驟

310 步驟

320 步驟

325 步驟

330 步驟

340 步驟

350 步驟

360 步驟

申請專利範圍

1. 一種設備，其包括：

一非揮發性儲存器，其儲存識別符(ID)基本資料；及

一處理器，其經組態以：

驗證正在該設備上執行之一應用程式之一憑證，該憑證含有用於該應用程式之一程式碼簽章者之一程式碼簽章者ID；

接收該應用程式之一唯一ID之一請求；

自該程式碼簽章者ID及該ID基本資料產生該唯一ID；及

傳回該所產生的唯一ID。

2. 如請求項1之設備，其中自該應用程式接收該唯一ID之該請求，且其中將該所產生的唯一ID傳回至該應用程式。

3. 如請求項2之設備，其中該ID基本資料係裝置所特有。

4. 如請求項3之設備，其中該唯一ID係藉由組合該程式碼簽章者ID與該ID基本資料及自該組合計算一單向雜湊函數而產生。

5. 如請求項4之設備，其中該唯一ID係藉由以下各者而產生：採用該程式碼簽章者ID作爲一字串、附加該ID基本資料至該字串及計算所得字串之一雜湊值。

6. 如請求項1之設備，其中該非揮發性儲存器亦儲存金鑰基本資料，且該處理器經進一步組態以：

自該應用程式接收一密碼編譯操作之一請求；

自該程式碼簽章者ID及該金鑰基本資料產生一加密金鑰；

使用該所產生的加密金鑰執行該所請求的密碼編譯操作；及

將該所請求的密碼編譯操作之一結果傳回至該應用程式。

7. 一種設備，其包括：

一非揮發性儲存器，其儲存金鑰基本資料；及

一處理器，其經組態以：

驗證正在該設備上執行之一應用程式之一憑證，該憑證含有用於該應用程式之一程式碼簽章者之一程式碼簽章者識別碼(ID)；

接收一密碼編譯操作之一請求；及

自該程式碼簽章者ID及該金鑰基本資料產生一加密金鑰。

8. 如請求項7之設備，其中自該應用程式接收該密碼編譯操作之該請求。

9. 如請求項7之設備，其中該金鑰基本資料係裝置所特有。

10. 如請求項7之設備，其中該所請求的密碼編譯操作係使用一私密金鑰加密或解密一訊息。

11. 如請求項7之設備，其中該所請求的密碼編譯操作係使用一對稱金鑰加密或解密一訊息。

12. 如請求項7之設備，其中該加密金鑰係藉由以下各者而產生：組合該程式碼簽章者ID與該金鑰基本資料、添加一密碼編譯salt值，且接著計算所得組合之一單向雜湊值。

13. 如請求項7之設備，其中該處理器經進一步組態以：

使用所產生的加密金鑰執行該所請求的密碼編譯操作；及

將該所請求的密碼編譯操作之一結果傳回至該應用程式。

14. 如請求項12之設備，其中該處理器經進一步組態以：

判定該所產生的加密金鑰爲弱；

若判定該加密金鑰爲弱，則使用一不同的密碼編譯salt值產生另一加密金鑰；及

判定該最近產生的加密金鑰是否爲弱。

15. 如請求項7之設備，其中該處理器經進一步組態以將一公開金鑰/私密金鑰對之一公開金鑰傳回至該應用程式。

16. 如請求項7之設備，其進一步包括儲存已產生的加密金鑰之一金鑰快取區。

17. 如請求項16之設備，其中該處理器經進一步組態以搜尋該金鑰快取區以判定該所請求的密碼編譯操作所需之一加密金鑰是否已儲存在該金鑰快取區中。

18. 如請求項7之設備，其中該非揮發性儲存器亦儲存ID基本資料，且該處理器經進一步組態以：

接收該應用程式之一唯一ID之一請求；

自該程式碼簽章者ID及該ID基本資料產生該唯一ID；及

將該所產生的唯一ID傳回至該應用程式。

19. 一種電腦實施方法，其包括：

在一設備之一非揮發性儲存器中儲存識別符(ID)基本資料；

驗證正在該設備上執行之一應用程式之一憑證，該憑證含有用於該應用程式之一程式碼簽章者之一程式碼簽章者ID；

接收該應用程式之一唯一ID之一請求；

自該程式碼簽章者ID及該ID基本資料產生該唯一ID；及

傳回該所產生的唯一ID。

20. 如請求項19之電腦實施方法，其中自該應用程式接收該唯一ID之該請求，且其中將該所產生的唯一ID傳回至該應用程式。

21. 如請求項20之電腦實施方法，其中該ID基本資料係裝置所特有。

22. 如請求項21之電腦實施方法，其中產生該唯一ID包含組合該程式碼簽章者ID與該ID基本資料及自該組合計算一單向雜湊函數。

23. 如請求項22之電腦實施方法，其中產生該唯一ID包含採用該程式碼簽章者ID作爲一字串、附加該ID基本資料至該字串及計算

所得字串之一雜湊值。

24. 如請求項19之電腦實施方法，其進一步包括：

在該非揮發性儲存器中儲存金鑰基本資料；

自該應用程式接收一密碼編譯操作之一請求；

自該程式碼簽章者ID及該金鑰基本資料產生一加密金鑰；

使用該所產生的加密金鑰執行該所請求的密碼編譯操作；及

將該所請求的密碼編譯操作之一結果傳回至該應用程式。

25. 一種電腦實施方法，其包括：

在一設備之一非揮發性儲存器中儲存金鑰基本資料；

驗證正在該設備上執行之一應用程式之一憑證，該憑證含有用於該應用程式之一程式碼簽章者之一程式碼簽章者ID；

接收一密碼編譯操作之一請求；及

自該程式碼簽章者ID及該金鑰基本資料產生一加密金鑰。

26. 如請求項25之電腦實施方法，其中自該應用程式接收該密碼編譯操作之該請求。

27. 如請求項25之電腦實施方法，其中該金鑰基本資料係裝置所特有。

28. 如請求項25之電腦實施方法，其中該所請求的密碼編譯操作係使用一私密金鑰加密或解密一訊息。

29. 如請求項25之電腦實施方法，其中該所請求的密碼編譯操作係使用一對稱金鑰加密或解密一訊息。

30. 如請求項25之電腦實施方法，其中產生該加密金鑰包含：組合該程式碼簽章者ID與該金鑰基本資料、添加一密碼編譯salt值及接著自所得組合計算一單向雜湊值。

31. 如請求項25之電腦實施方法，其進一步包括：

使用該所產生的加密金鑰執行該所請求的密碼編譯操作；及

將該所請求的密碼編譯操作之一結果傳回至該應用程式。

32. 如請求項30之電腦實施方法，其進一步包括：

判定該所產生的加密金鑰爲弱；

若判定該加密金鑰爲弱，則使用一不同的密碼編譯salt值產生另一加密金鑰；及

判定最近產生的加密金鑰是否爲弱。

33. 如請求項25之電腦實施方法，其進一步包括將一公開金鑰/私密金鑰對之一公開金鑰傳回至該應用程式。

34. 如請求項25之電腦實施方法，其進一步包括將已產生的加密金鑰儲存在該設備之一金鑰快取區。

35. 如請求項34之電腦實施方法，其進一步包括搜尋該金鑰快取區以判定該所請求的密碼編譯操作所需之一加密金鑰是否已儲存在該金鑰快取區中。

36. 如請求項25之電腦實施方法，其進一步包括：

在該非揮發性儲存器中儲存ID基本資料；

接收該應用程式之一唯一ID之一請求；

自該程式碼簽章者ID及該ID基本資料產生該唯一ID；及

將該所產生的唯一ID傳回至該應用程式。

圖式

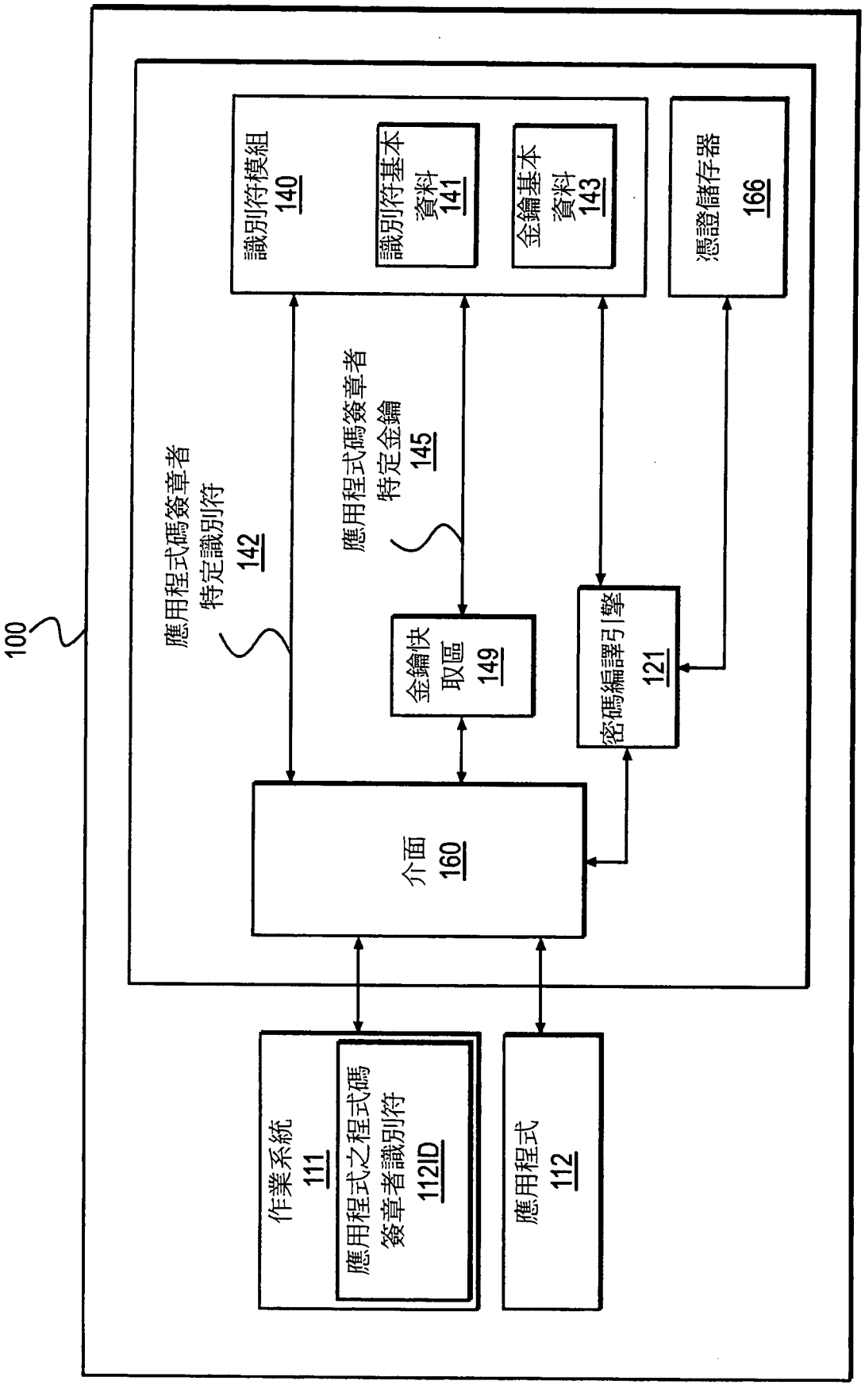
100
識別符模組
140
識別符基本資料
141
金鑰基本資料
143
憑證儲存器
166
應用程式碼簽章者特定識別符
142
應用程式碼簽章者特定金鑰
145
金鑰快取區
149
密碼編譯引擎
121
介面
160
作業系統
111
應用程式之程式碼簽章者識別符
112ID
應用程式
112

圖1

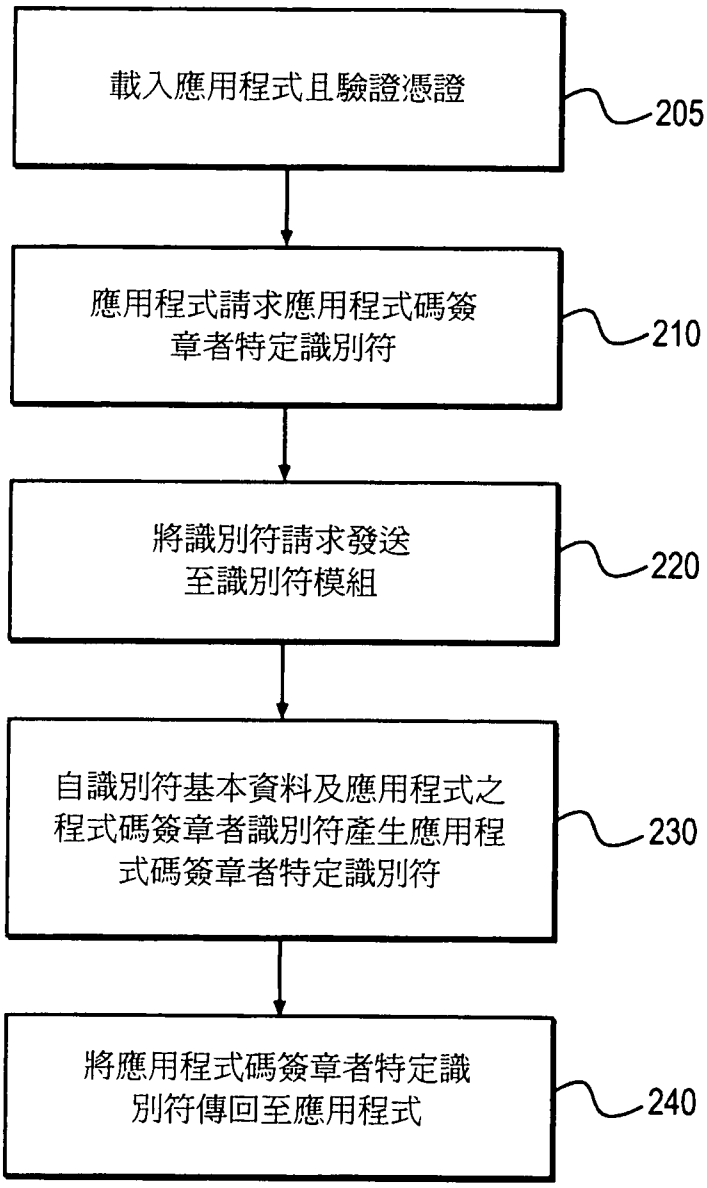
載入應用程式且驗證憑證
205
應用程式請求應用程式碼簽章者特定識別符
210
將識別符請求發送至識別符模組
220
自識別符基本資料及應用程式之程式碼簽章者識別符產生應用程式碼簽章者特定識別符
230
將應用程式碼簽章者特定識別符傳回至應用程式
240

圖2

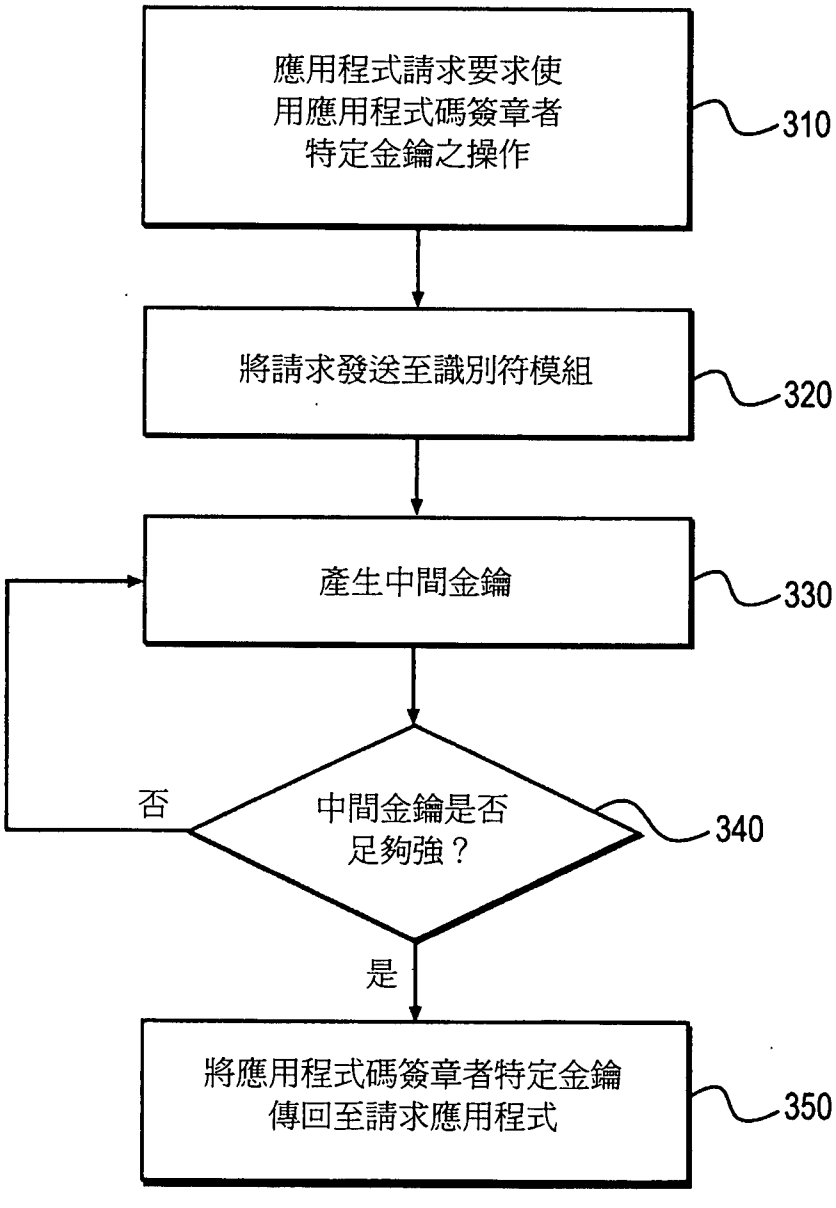
應用程式請求要求使用應用程式碼簽章者特定金鑰之操作
310
將請求發送至識別符模組
320
產生中間金鑰
330
中間金鑰是否足夠強？
340
否
是
將應用程式碼簽章者特定金鑰傳回至請求應用程式
350

圖3A

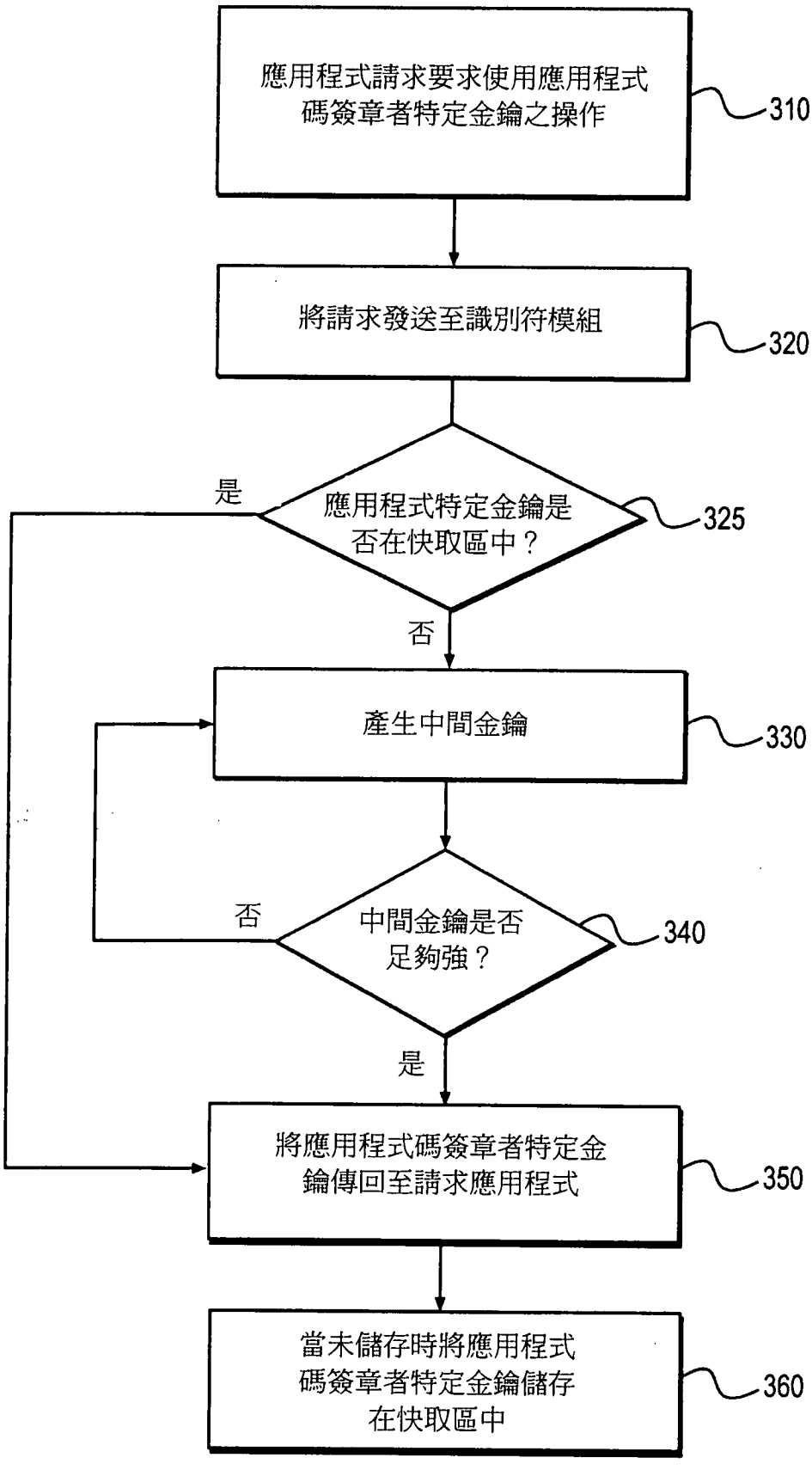
應用程式請求要求使用應用程式碼簽章者特定金鑰之操作
310
將請求發送至識別符模組
320
是
應用程式特定金鑰是否在快取區中？
325
否
產生中間金鑰
330
否
中間金鑰是否足夠強？
340
是
將應用程式碼簽章者特定金鑰傳回至請求應用程式
350
當未儲存時將應用程式碼簽章者特定金鑰儲存在快取區中
360

圖3B