I635409

(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 I635409 B**

(45)公告日： 中華民國 107 (2018) 年 09 月 11 日

(21)申請案號：106125986 (22)申請日： 中華民國 102 (2013) 年 12 月 27 日

(51)Int. Cl.： *G06F21/31 (2013.01)* *G06F21/60 (2013.01)*
G06F17/30 (2006.01)

(30)優先權：2012/12/28 美國 13/730,761
2012/12/28 美國 13/730,776
2012/12/28 美國 13/730,780
2012/12/28 美國 13/730,791
2012/12/28 美國 13/730,795

(71)申請人：諾克諾克實驗公司 (美國) NOK NOK LABS, INC. (US)
美國

(72)發明人：巴吉達薩拉亞達非特 BAGHDASARYAN,DAVIT (AM) ；勞瑞馬特 LOURIE,MATT (US) ；里得曼洛夫 LINDEMANN,ROLF (DE) ；威爾森伯多 J WILSON,BRENDON J. (US) ；伯西歐馬克 BRICENO,MARC (US) ；多拉奇亞拉捷夫 DHOLAKIA,RAJIV (US) ；娜葛拉珍娜葛 NAGARAJAN,NAGA (US)

(74)代理人：陳長文

(56)參考文獻：

TW	200701120A	TW	201121280A
US	20030115142A1	US	2011/0082801A1

審查人員：林彥廷

申請專利範圍項數：27 項 圖式數：16 共 64 頁

(54)名稱

判定認證能力之查詢系統、方法及非暫態機器可讀媒體

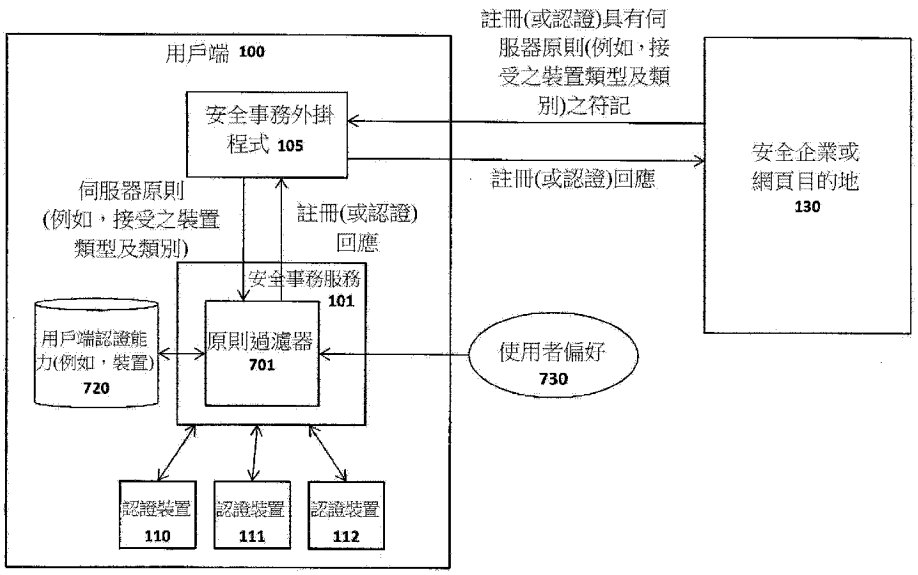
QUERY SYSTEM, METHOD AND NON-TRANSITORY MACHINE-READABLE MEDIUM TO DETERMINE AUTHENTICATION CAPABILITIES

(57)摘要

本發明闡述一種用於判定認證能力之系統、設備、方法及機器可讀媒體。舉例而言，一種方法之一項實施例包括：接收識別一組可接受認證能力之一原則；判定一組用戶端認證能力；且基於該組所判定用戶端認證能力過濾該組可接受認證能力以得出一組經過濾之一或多個認證能力用於認證該用戶端之一使用者。

A system, apparatus, method, and machine readable medium are described for determining the authentication capabilities. For example, one embodiment of a method comprises: receiving a policy identifying a set of acceptable authentication capabilities; determining a set of client authentication capabilities; and filtering the set of acceptable authentication capabilities based on the determined set of client authentication capabilities to arrive at a filtered set of one or more authentication capabilities for authenticating a user of the client.

指定代表圖：



【圖 7】

符號簡單說明：

100・・・用戶端

101・・・安全事務服務

105・・・瀏覽器外掛程式/安全事務外掛程式/外掛程式

110・・・認證裝置

111・・・認證裝置

112・・・認證裝置

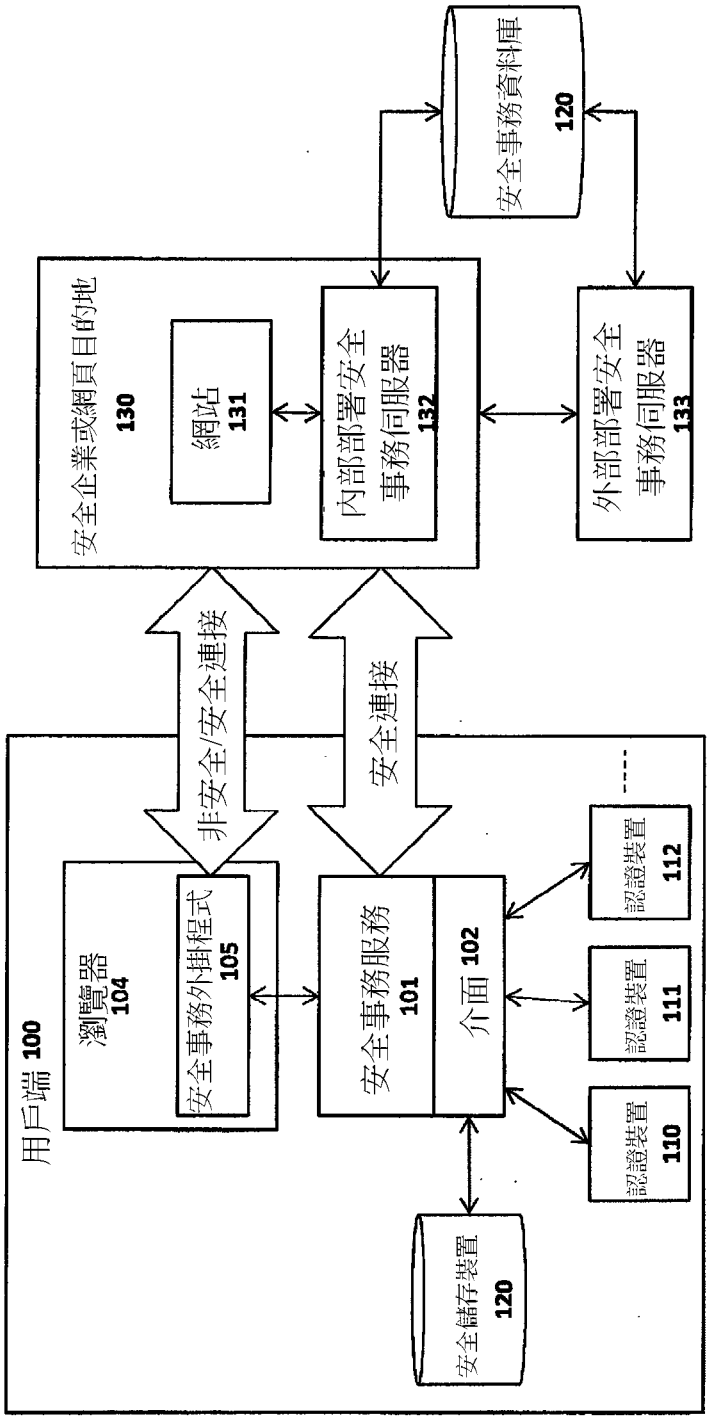
130・・・伺服器/安全企業或網頁目的地/認證裝置/安全事務服務

701・・・原則過濾器

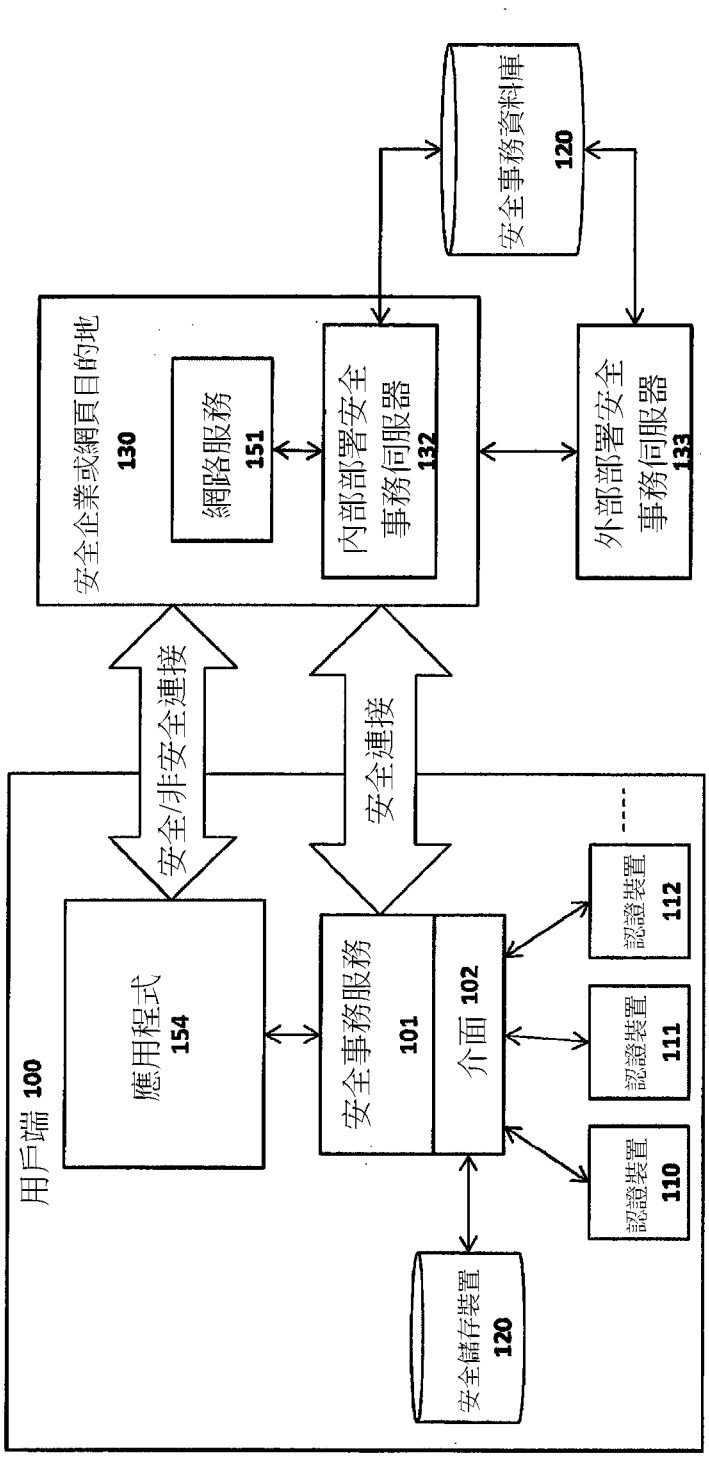
720・・・安全儲存區域/安全儲存裝置

730・・・使用者偏好

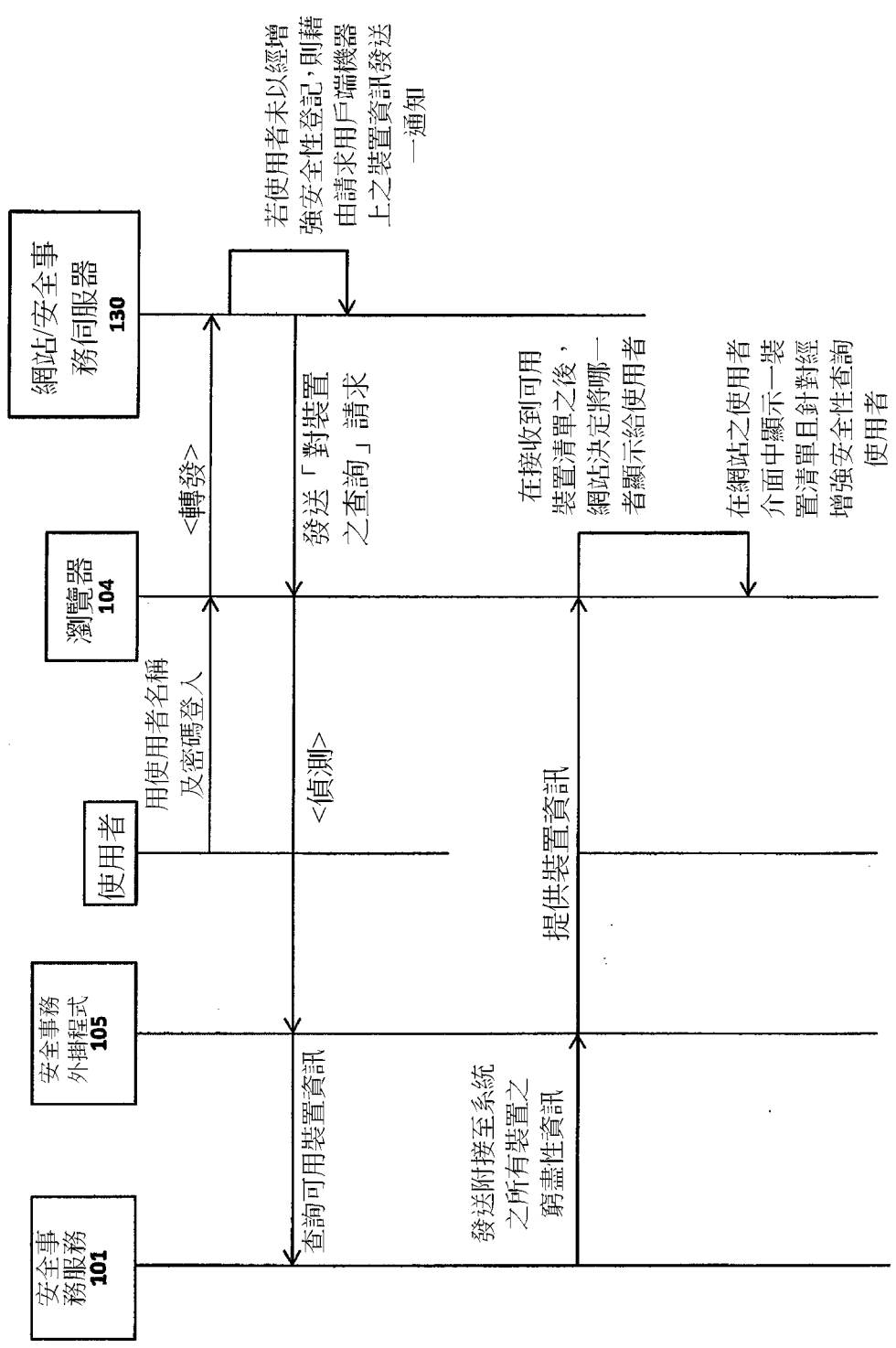
【發明圖式】


安全事務資料庫
120
安全企業或網頁目的地
130
網站
131
內部部署安全事務伺服器
132
外部部署安全事務伺服器
133
非安全/安全連接
安全連接
用戶端 100
瀏覽器
104
安全事務外掛程式
105
安全事務服務
101
介面 102
認證裝置
112
認證裝置
111
認證裝置
110
安全儲存裝置
120

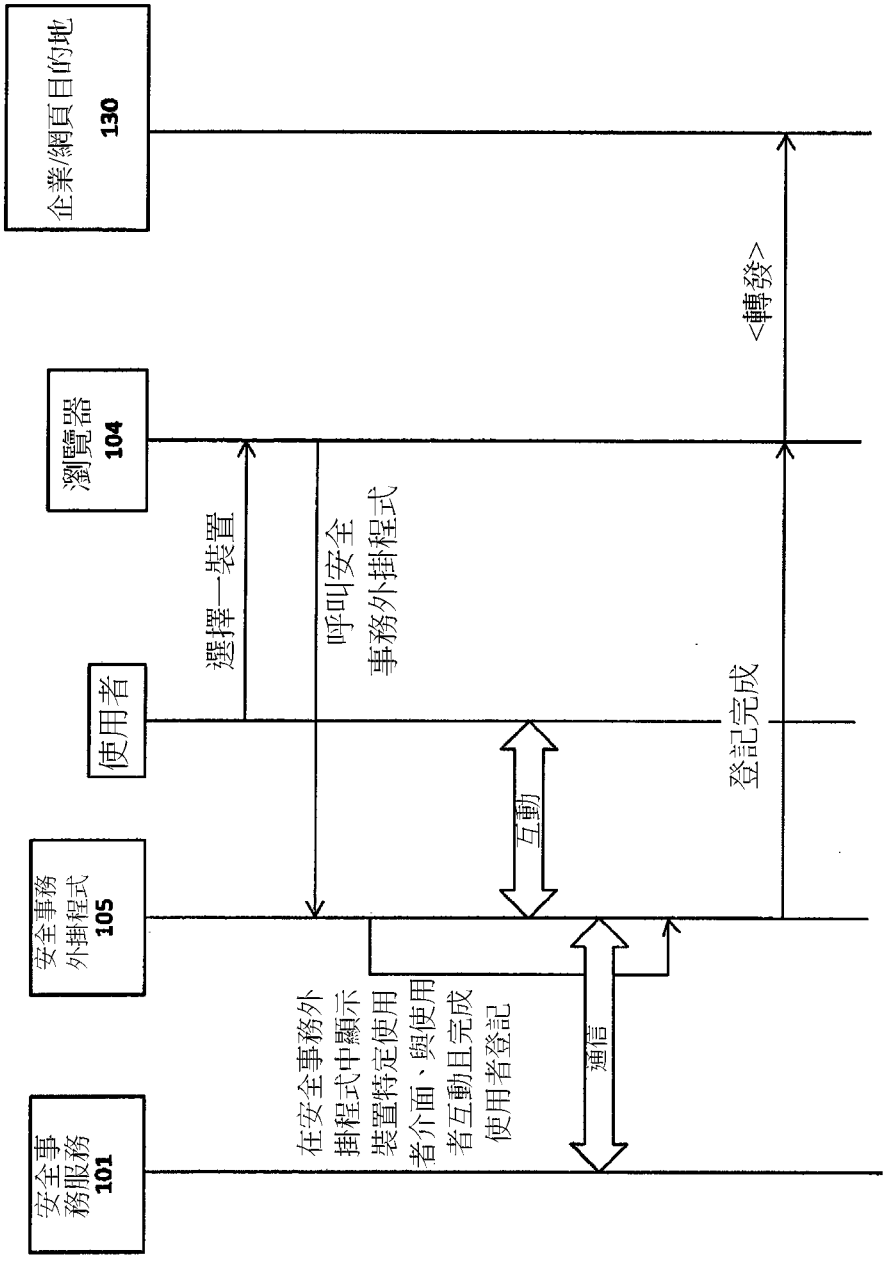
【圖 1A】


安全事務資料庫
120
安全企業或網頁目的地
130
網路服務
151
內部部署安全
事務伺服器
132
外部部署安全
事務伺服器
133
安全/非安全連接
安全連接
用戶端 100
應用程式
154
安全事務服務
101
介面 102
認證裝置
112
認證裝置
111
認證裝置
110
安全儲存裝置
120

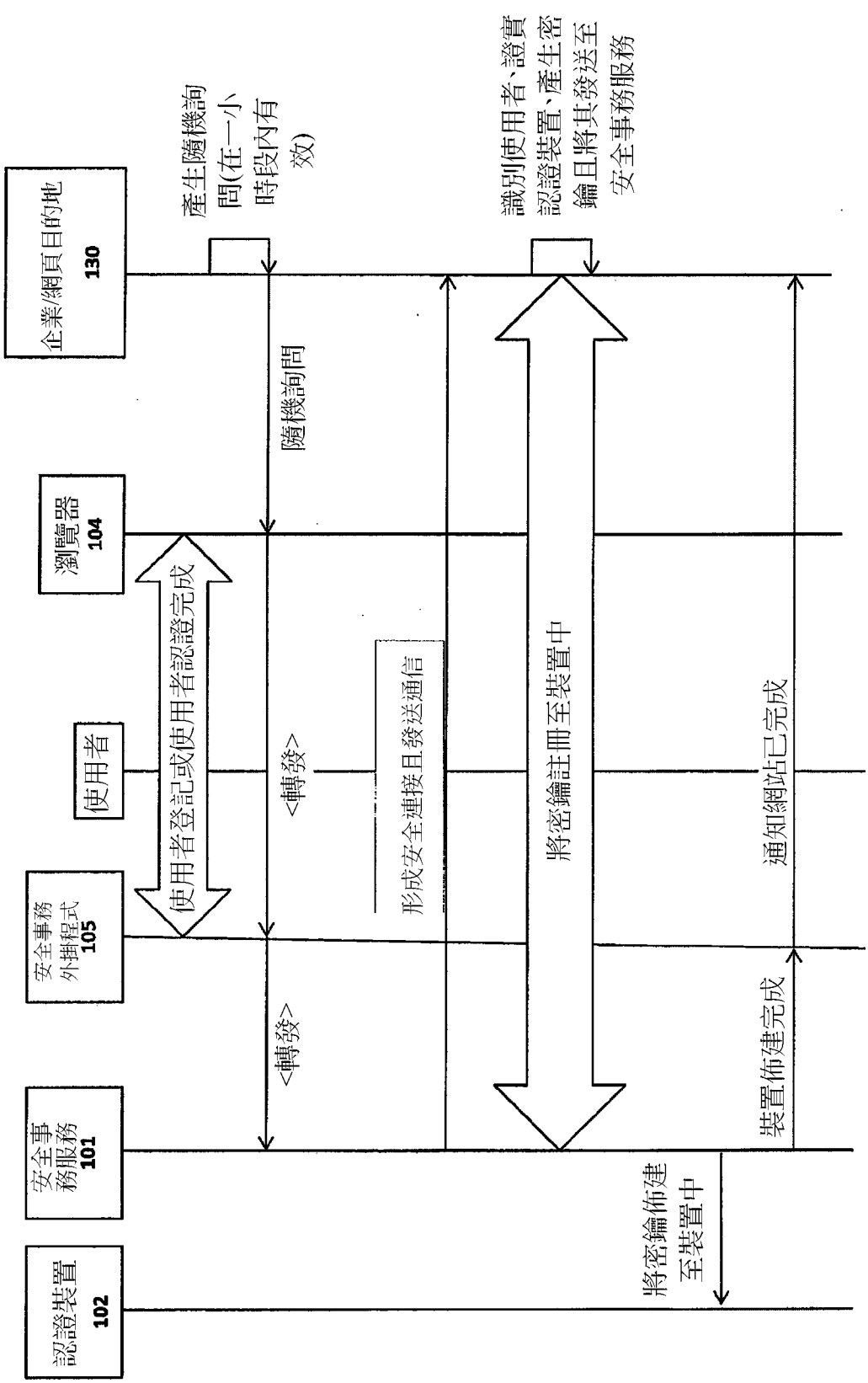
【圖 1B】


安全事務服務 101
安全事務外掛程式 105
使用者
瀏覽器 104
網站/安全事務伺服器 130
用使用者名稱及密碼登入
<偵測>
<轉發>
查詢可用裝置資訊
發送附接至系統之所有裝置之窮盡性資訊
提供裝置資訊
發送「對裝置之查詢」請求
若使用者未以經增強安全性登記，則藉由請求用戶端機器上之裝置資訊發送一通知
在接收到可用裝置清單之後，網站決定將哪一者顯示給使用者
在網站之使用者介面中顯示一裝置清單且針對經增強安全性查詢使用者

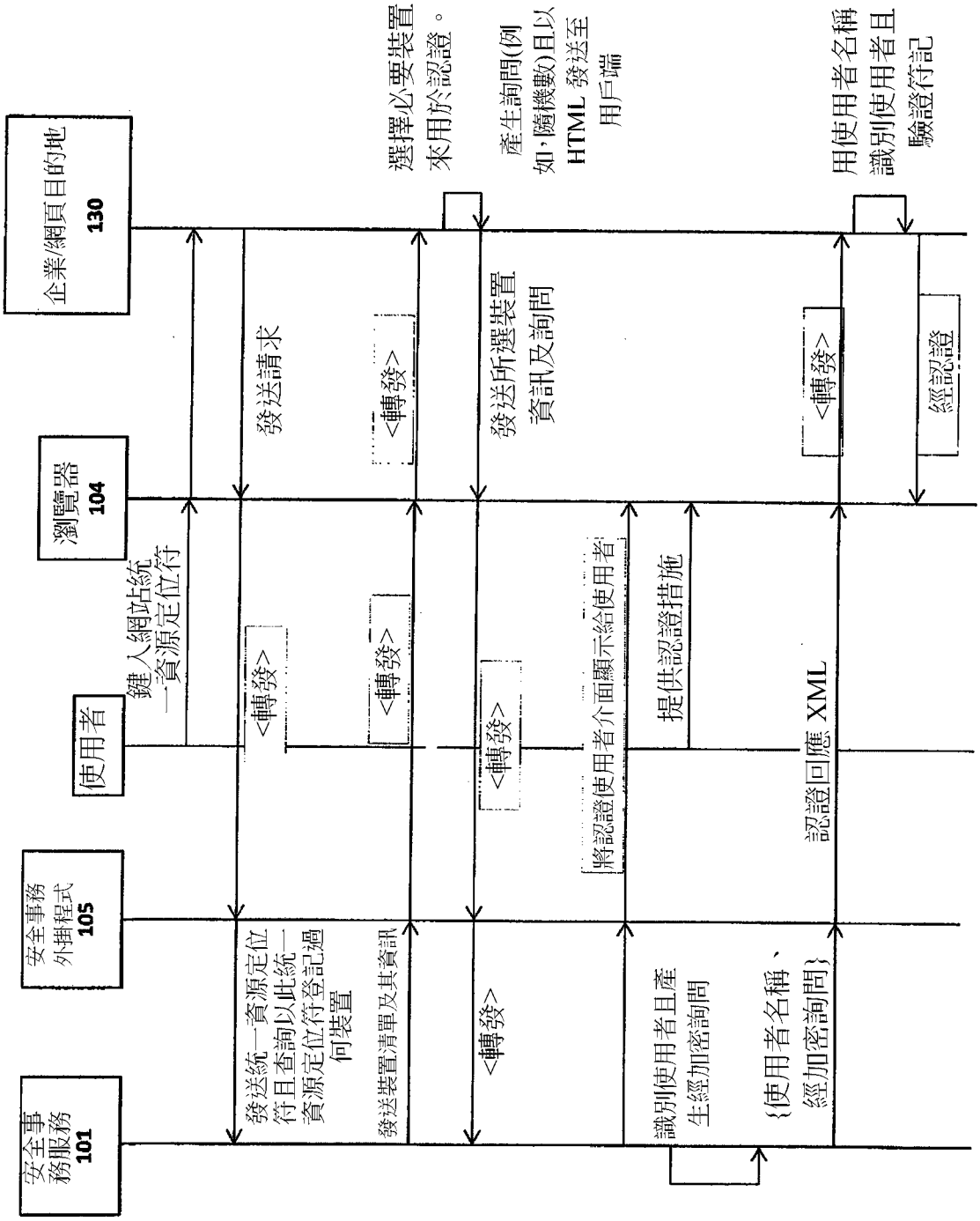
【圖 2】


企業/網頁目的地
130
瀏覽器
104
使用者
安全事務
外掛程式
105
安全事務
務服務
101
<轉發>
選擇一裝置
呼叫安全
事務外掛程式
互動
登記完成
在安全事務外
掛程式中顯示
裝置特定使用
者介面、與使用
者互動且完成
使用者登記
通信

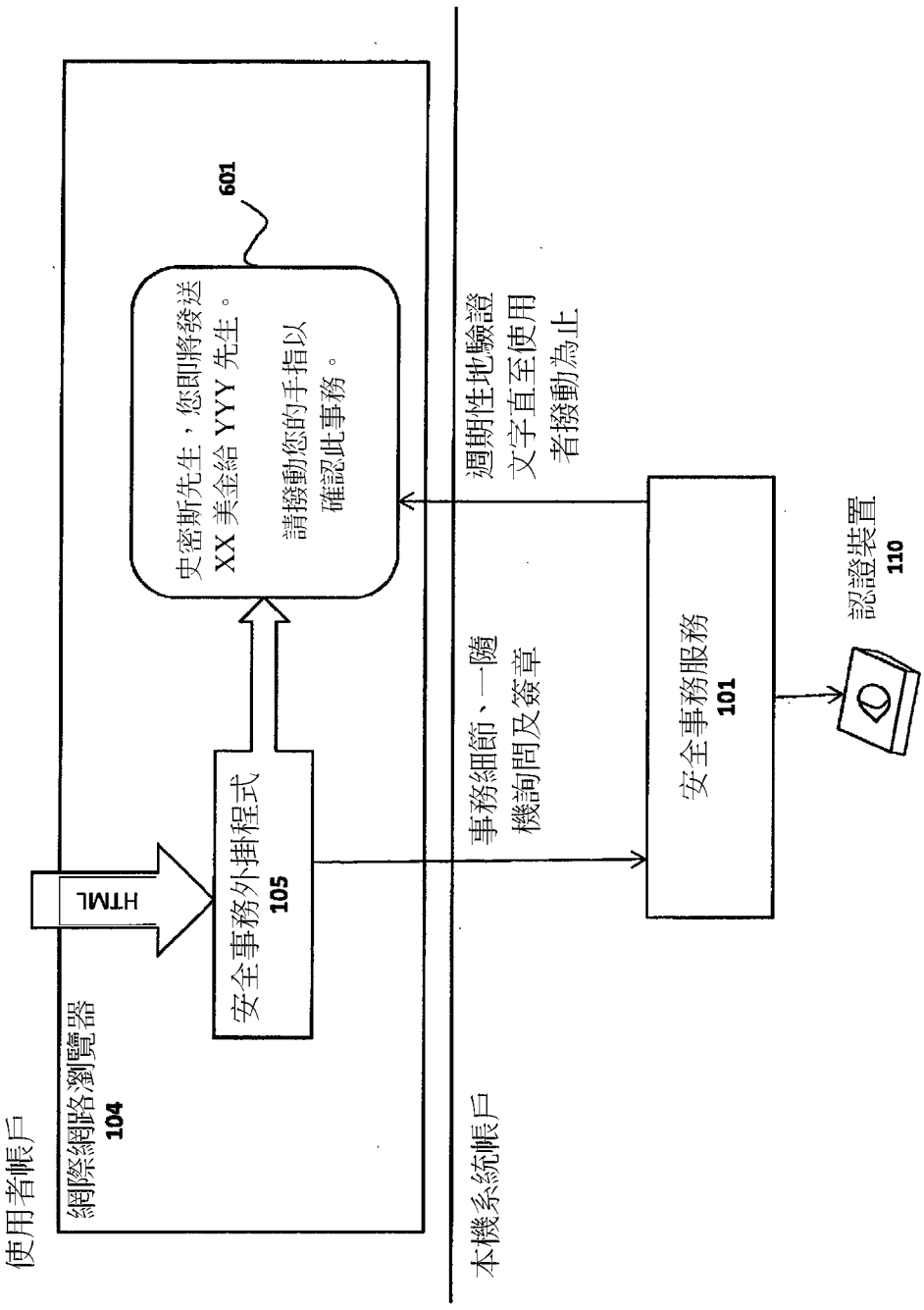
【圖 3】


企業/網頁目的地
130
產生隨機詢問(在一小時段內有效)
識別使用者、證實認證裝置、產生密鑰且將其發送至安全事務服務
瀏覽器
104
隨機詢問
使用者
使用者登記或使用者認證完成
<轉發>
形成安全連接且發送通信
將密鑰註冊至裝置中
通知網站已完成
安全事務外掛程式
105
<轉發>
裝置佈建完成
安全事務服務
101
將密鑰佈建至裝置中
認證裝置
102

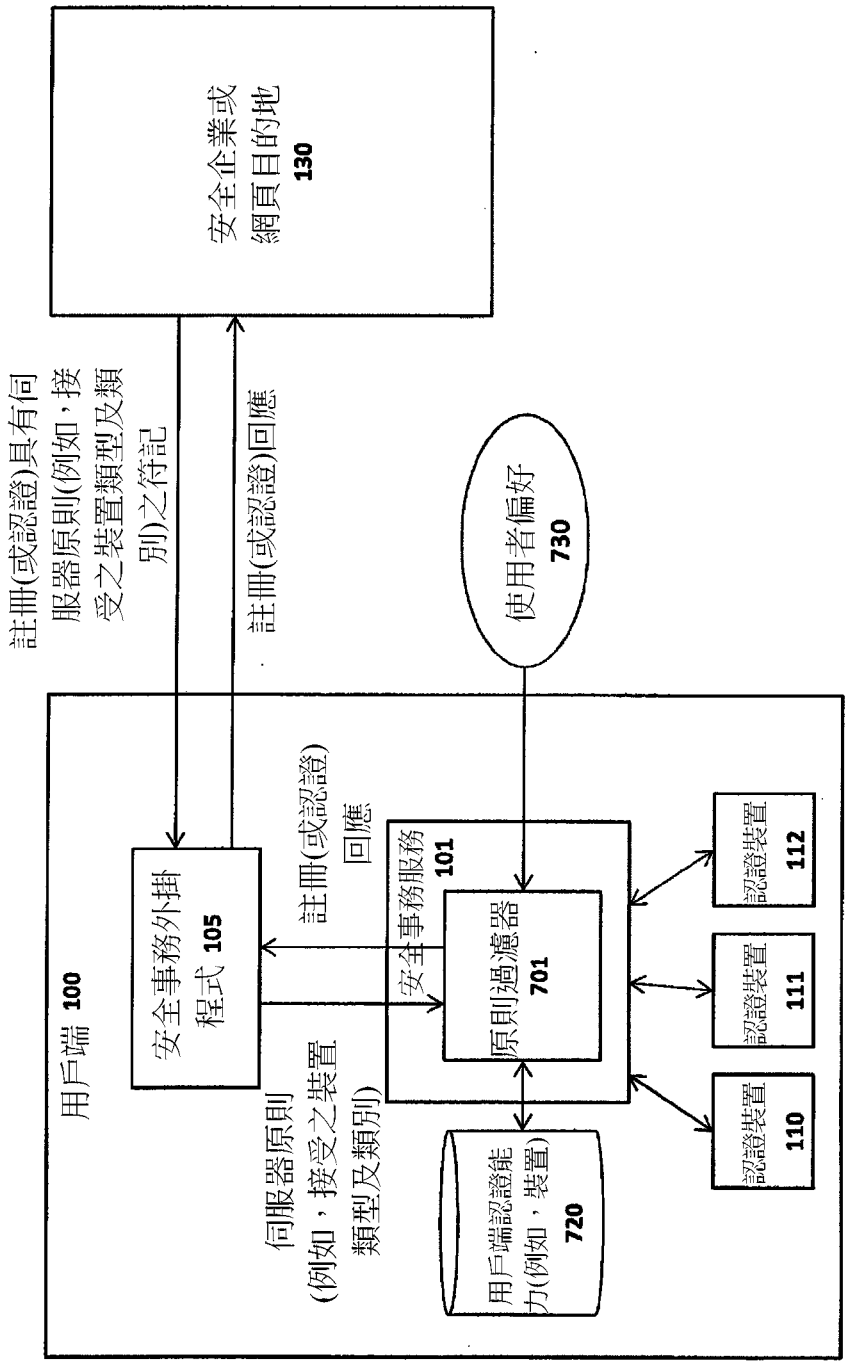
【圖 4】


安全事務服務 101
安全事務外掛程式 105
使用者
瀏覽器 104
企業/網頁目的地 130
鍵入網站統一資源定位符
發送請求
<轉發>
選擇必要裝置來用於認證。
產生詢問(例如，隨機數)且以 HTML 發送至用戶端
發送所選裝置資訊及詢問
發送統一資源定位符且查詢以此統一資源定位符登記過何裝置
發送裝置清單及其資訊
將認證使用者介面顯示給使用者
提供認證措施
識別使用者且產生經加密詢問
{使用者名稱、經加密詢問}
認證回應 XML
用使用者名稱識別使用者且驗證符記
經認證

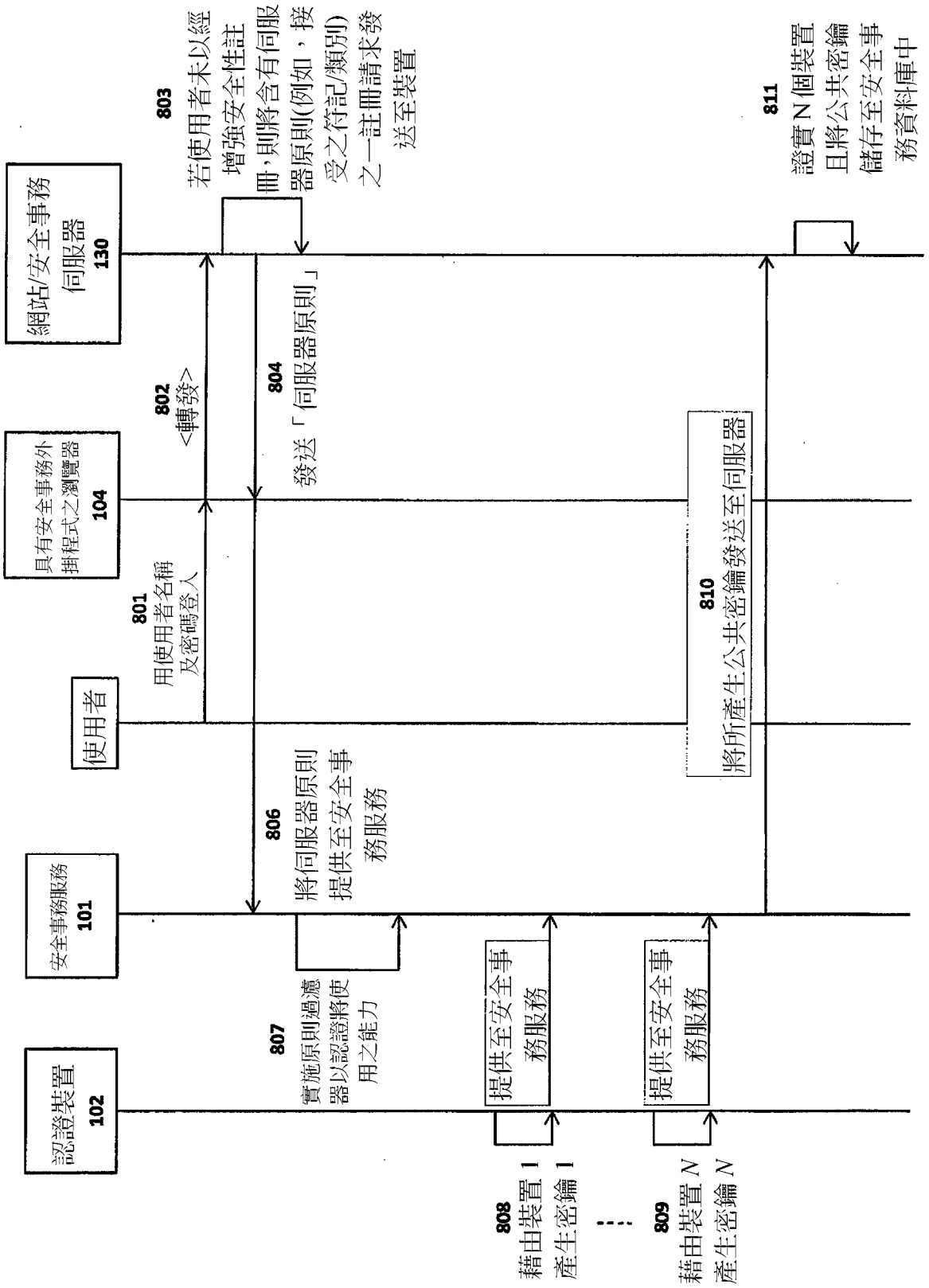
【圖 5】


使用者帳戶
網際網路瀏覽器
104
HTML
安全事務外掛程式
105
601
史密斯先生，您即將發送
XX 美金給 YYY 先生。
請撥動您的手指以
確認此事務。
本機系統帳戶
事務細節、一隨
機詢問及簽章
週期性地驗證
文字直至使用
者撥動為止
安全事務服務
101
認證裝置
110

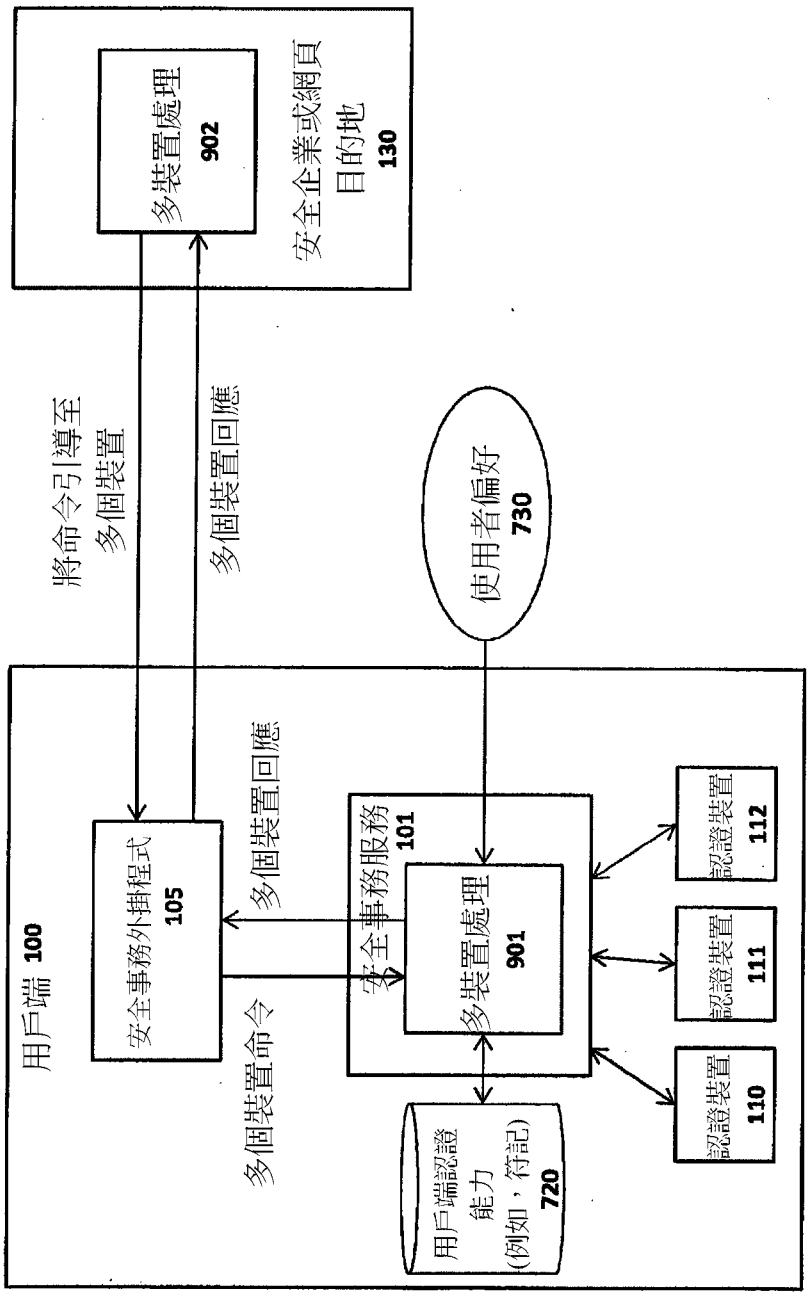
【圖 6】


安全企業或
網頁目的地
130
註冊(或認證)具有伺
服器原則(例如，接
受之裝置類型及類
別)之符記
註冊(或認證)回應
使用者偏好
730
用戶端 100
安全事務外掛
程式 105
註冊(或認證)
回應
安全事務服務
101
原則過濾器
701
伺服器原則
(例如，接受之裝置
類型及類別)
用戶端認證能
力(例如，裝置)
720
認證裝置
110
認證裝置
111
認證裝置
112

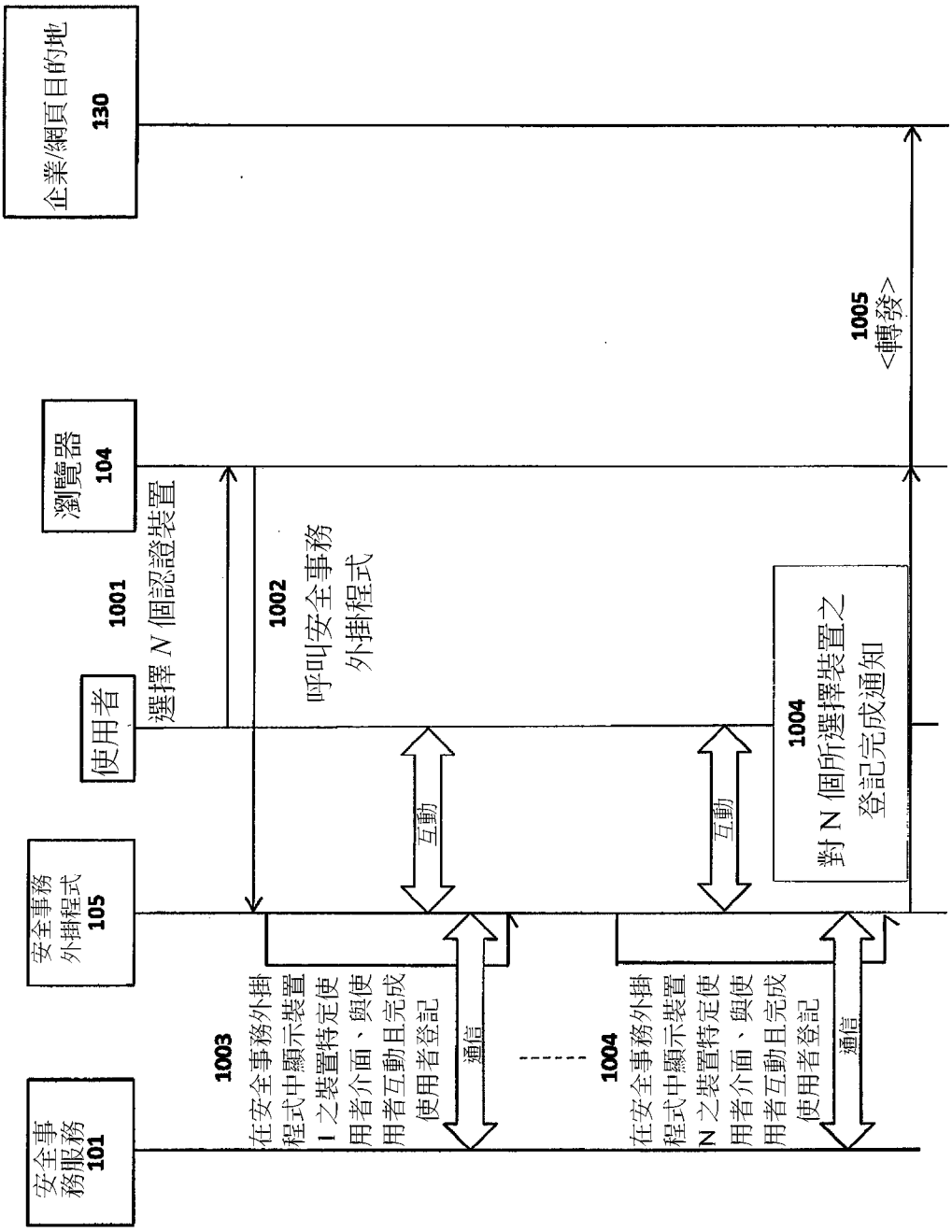
【圖 7】


網站/安全事務伺服器 130
具有安全事務外掛程式之瀏覽器 104
使用者
安全事務服務 101
認證裝置 102
803 若使用者未以經增強安全性註冊，則將含有伺服器原則(例如，接受之符記/類別)之一註冊請求發送至裝置
802 <轉發>
804 發送「伺服器原則」
801 用使用者名稱及密碼登入
806 將伺服器原則提供至安全事務服務
807 實施原則過濾器以認證將使用之能力
808 藉由裝置 1 產生密鑰 1
809 藉由裝置 N 產生密鑰 N
提供至安全事務服務
提供至安全事務服務
810 將所產生公共密鑰發送至伺服器
811 證實 N 個裝置且將公共密鑰儲存至安全事務資料庫中

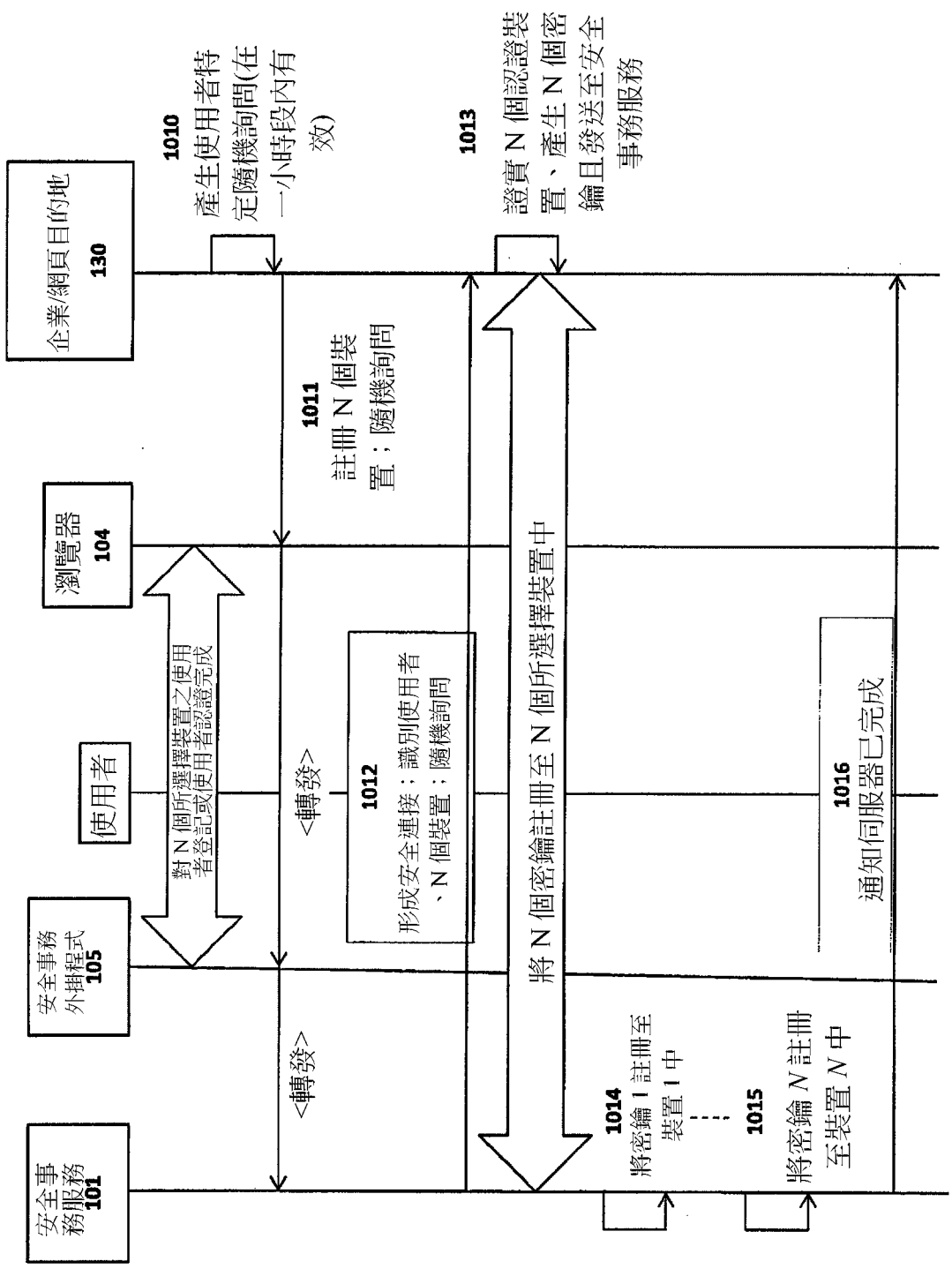
【圖 8】


安全企業或網頁目的地 130
多裝置處理 902
將命令引導至多個裝置
多個裝置回應
使用者偏好 730
用戶端 100
安全事務外掛程式 105
多個裝置回應
多個裝置命令
安全事務服務 101
多裝置處理 901
認證裝置 112
認證裝置 111
認證裝置 110
用戶端認證能力(例如，符記) 720

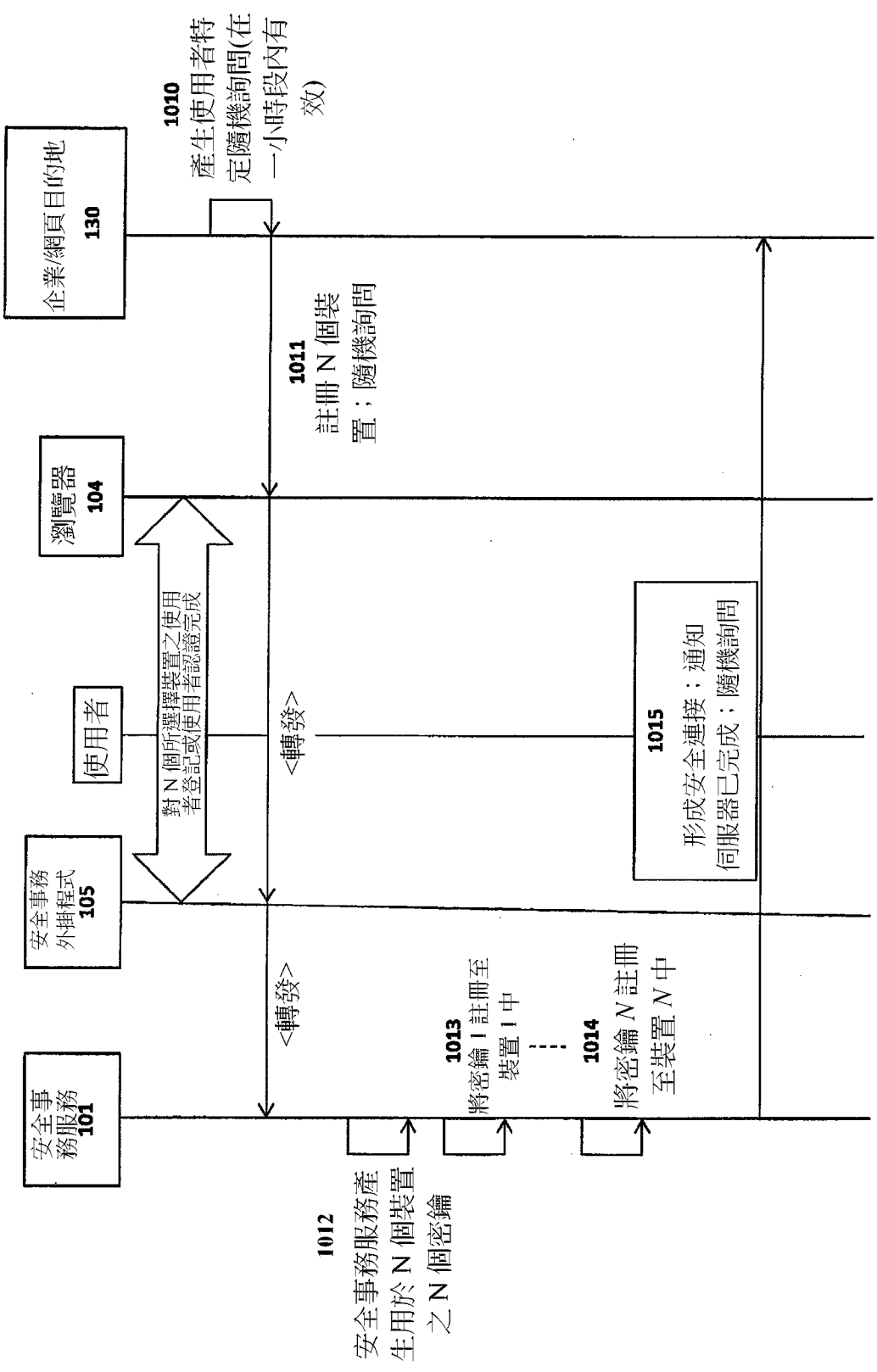
【圖 9】


企業/網頁目的地
130
瀏覽器
104
使用者
1001
選擇 N 個認證裝置
1002
呼叫安全事務
外掛程式
安全事務
外掛程式
105
互動
互動
1004
對 N 個所選擇裝置之
登記完成通知
1005
<轉發>
安全事務
服務
101
1003
在安全事務外掛
程式中顯示裝置
1 之裝置特定使
用者介面、與使
用者互動且完成
使用者登記
通信
1004
在安全事務外掛
程式中顯示裝置
N 之裝置特定使
用者介面、與使
用者互動且完成
使用者登記
通信

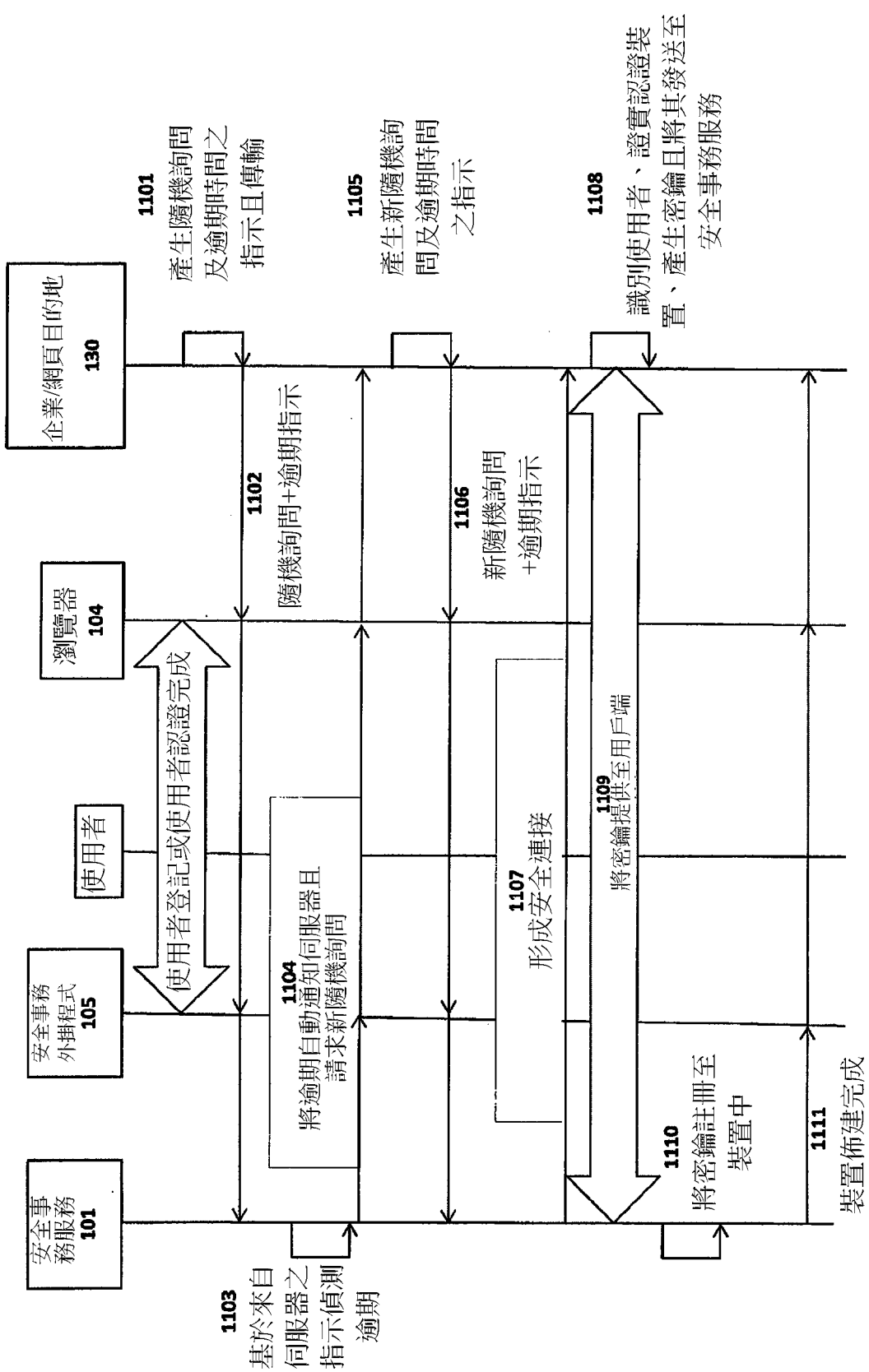
【圖 10A】


企業/網頁目的地
130
1010
產生使用者特定隨機詢問(在一小時段內有效)
1013
證實 N 個認證裝置、產生 N 個密鑰且發送至安全事務服務
瀏覽器
104
1011
註冊 N 個裝置；隨機詢問
使用者
對 N 個所選擇裝置之使用者登記或使用者認證完成
<轉發>
1012
形成安全連接；識別使用者、N 個裝置；隨機詢問
安全事務外掛程式
105
將 N 個密鑰註冊至 N 個所選擇裝置中
1016
通知伺服器已完成
安全事務服務
101
<轉發>
1014
將密鑰 1 註冊至裝置 1 中
1015
將密鑰 N 註冊至裝置 N 中

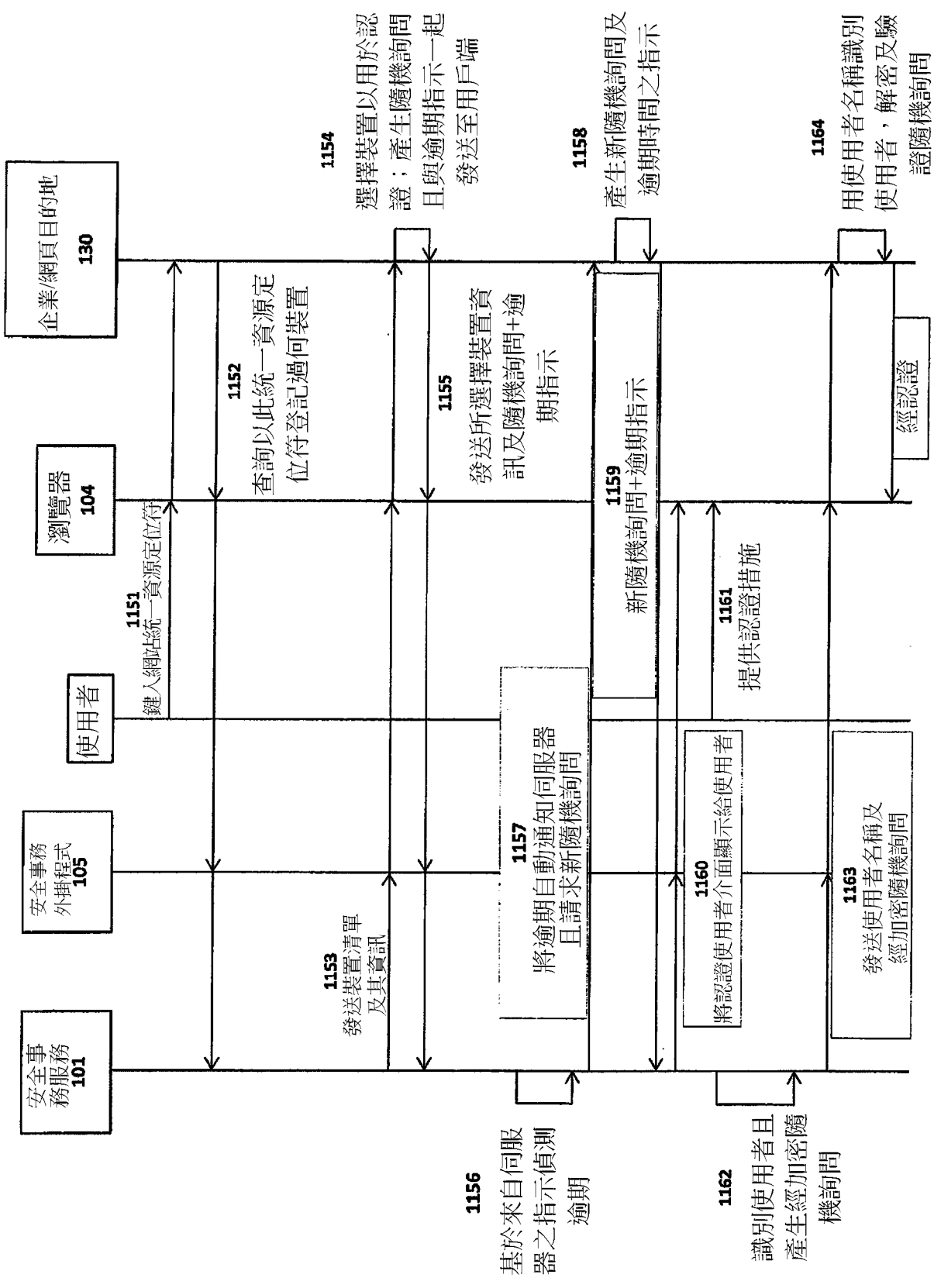
【圖 10B】


企業/網頁目的地
130
1010
產生使用者特定隨機詢問(在一小時段內有效)
瀏覽器
104
1011
註冊 N 個裝置；隨機詢問
使用者
對 N 個所選擇裝置之使用者登記或使用者認證完成
安全事務外掛程式
105
<轉發>
1015
形成安全連接；通知伺服器已完成；隨機詢問
安全事務服務
101
<轉發>
1013
將密鑰 1 註冊至裝置 1 中
1014
將密鑰 N 註冊至裝置 N 中
1012
安全事務服務產生用於 N 個裝置之 N 個密鑰

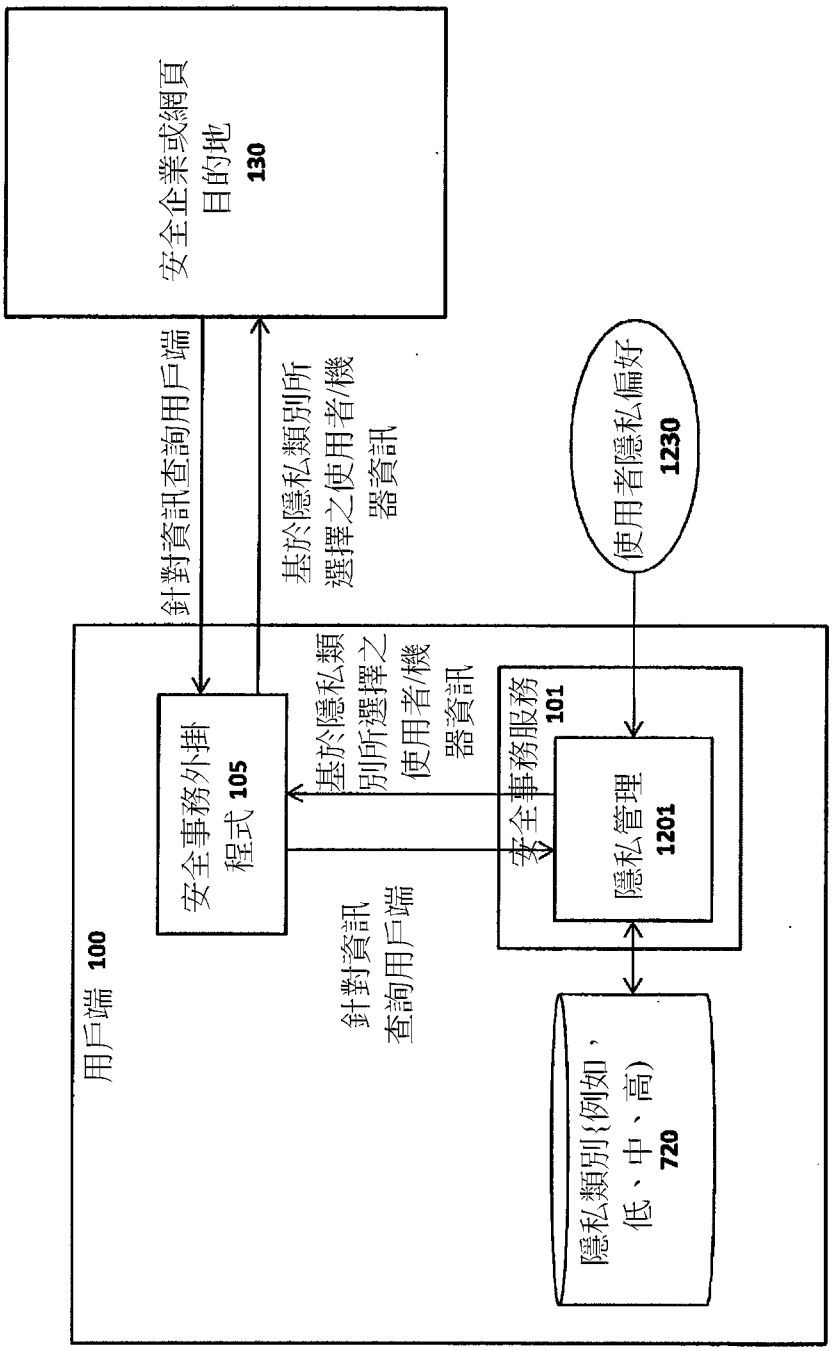
【圖 10C】


企業/網頁目的地
130
瀏覽器
104
使用者
安全事務
外掛程式
105
安全事務
服務
101
1101
產生隨機詢問
及逾期時間之
指示且傳輸
1102
隨機詢問+逾期指示
1103
基於來自
伺服器之
指示偵測
逾期
使用者登記或使用者認證完成
1104
將逾期自動通知伺服器且
請求新隨機詢問
1105
產生新隨機詢
問及逾期時間
之指示
1106
新隨機詢問
+逾期指示
1107
形成安全連接
1108
識別使用者、證實認證裝
置、產生密鑰且將其發送至
安全事務服務
1109
將密鑰提供至用戶端
1110
將密鑰註冊至
裝置中
1111
裝置佈建完成

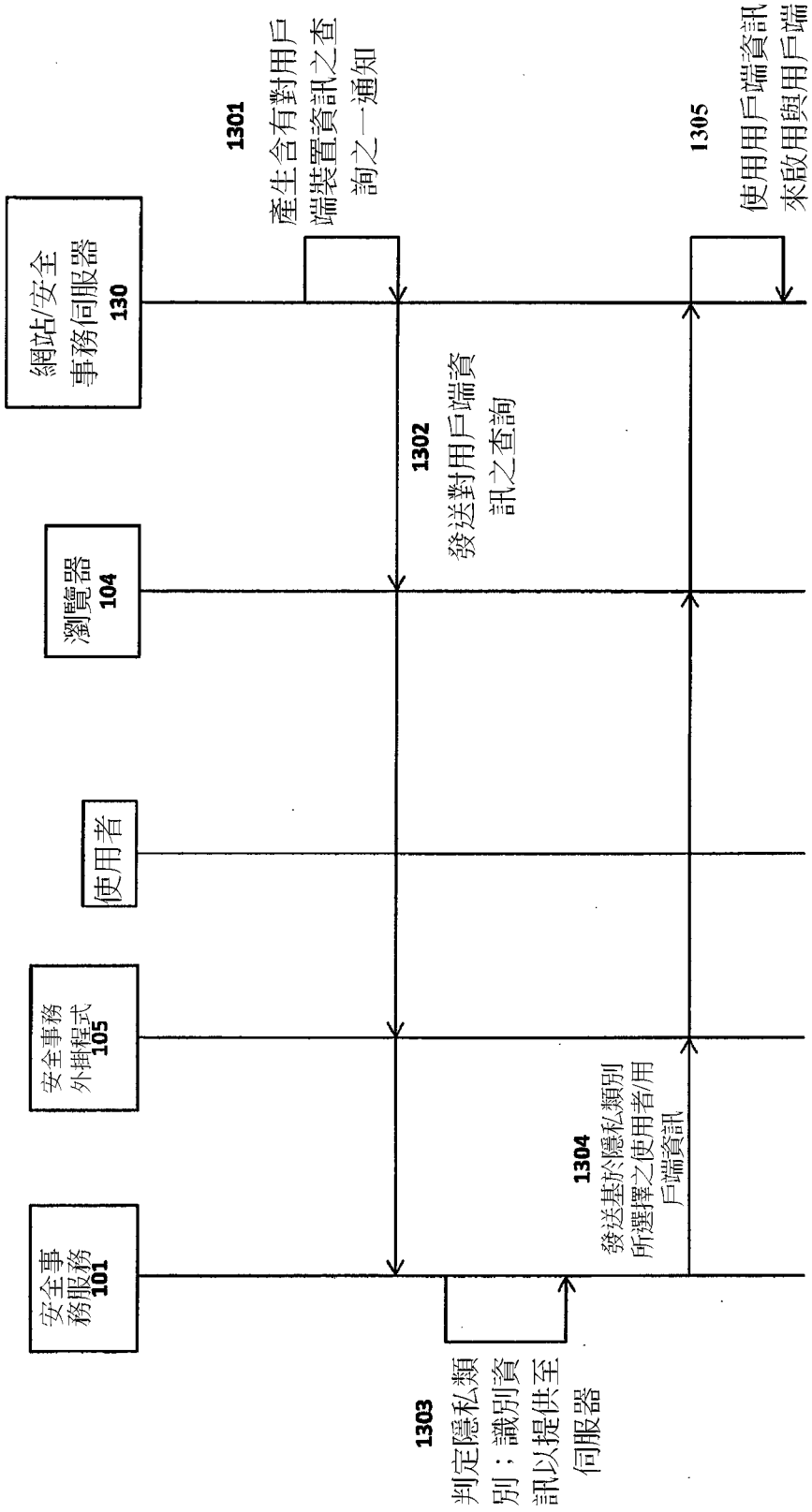
【圖 11A】


安全事務服務 101
安全事務外掛程式 105
使用者
瀏覽器 104
企業/網頁目的地 130
1151 鍵入網站統一資源定位符
1152 查詢以此統一資源定位符登記過何裝置
1153 發送裝置清單及其資訊
1154 選擇裝置以用於認證；產生隨機詢問且與逾期指示一起發送至用戶端
1155 發送所選擇裝置資訊及隨機詢問+逾期指示
1156 基於來自伺服器之指示偵測逾期
1157 將逾期自動通知伺服器且請求新隨機詢問
1158 產生新隨機詢問及逾期時間之指示
1159 新隨機詢問+逾期指示
1160 將認證使用者介面顯示給使用者
1161 提供認證措施
1162 識別使用者且產生經加密隨機詢問
1163 發送使用者名稱及經加密隨機詢問
1164 用使用者名稱識別使用者，解密及驗證隨機詢問
經認證

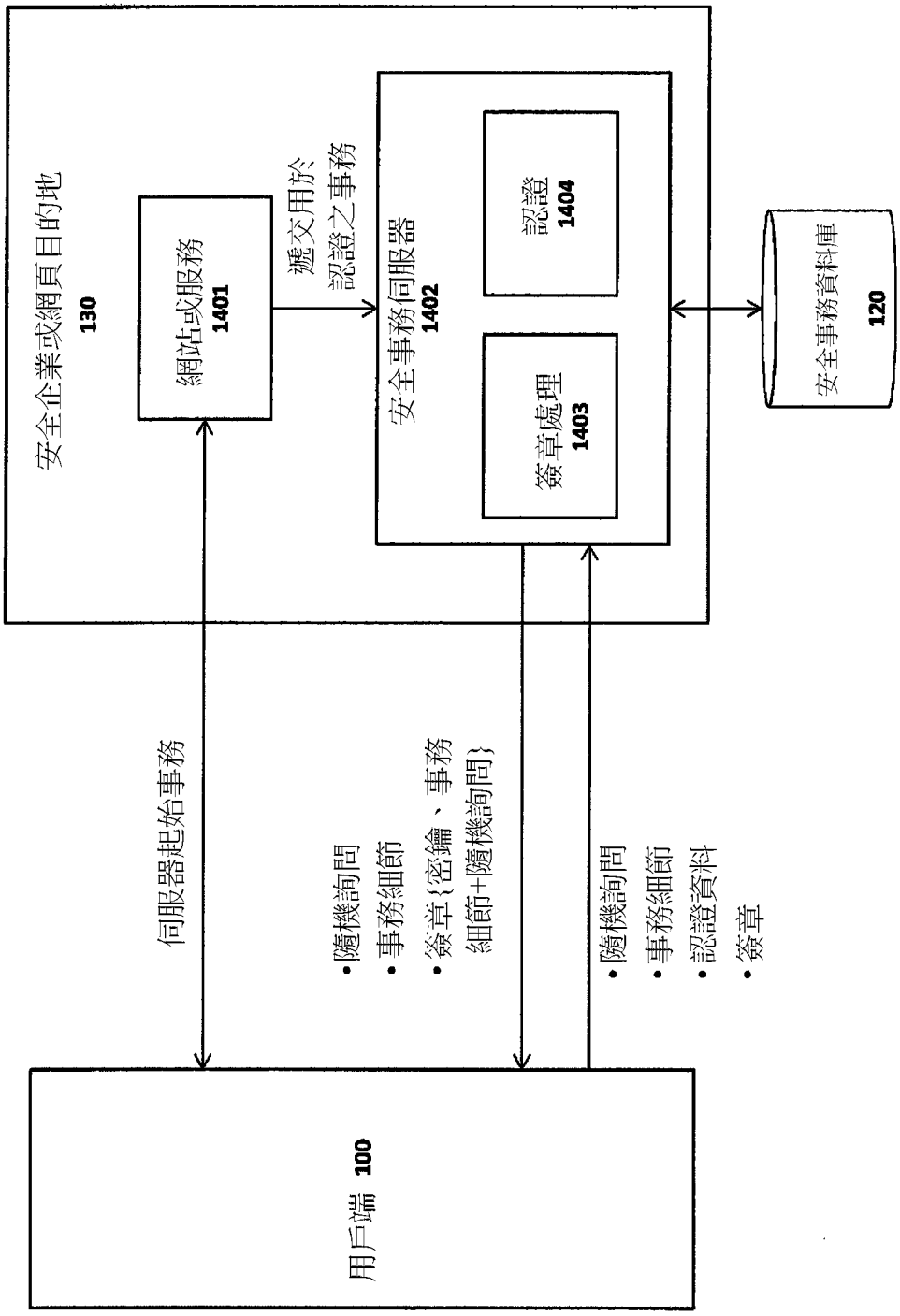
【圖 11B】


安全企業或網頁目的地 130
針對資訊查詢用戶端
基於隱私類別所選擇之使用者/機器資訊
使用者隱私偏好 1230
用戶端 100
安全事務外掛程式 105
基於隱私類別所選擇之使用者/機器資訊
針對資訊查詢用戶端
安全事務服務 101
隱私管理 1201
隱私類別{例如，低、中、高) 720

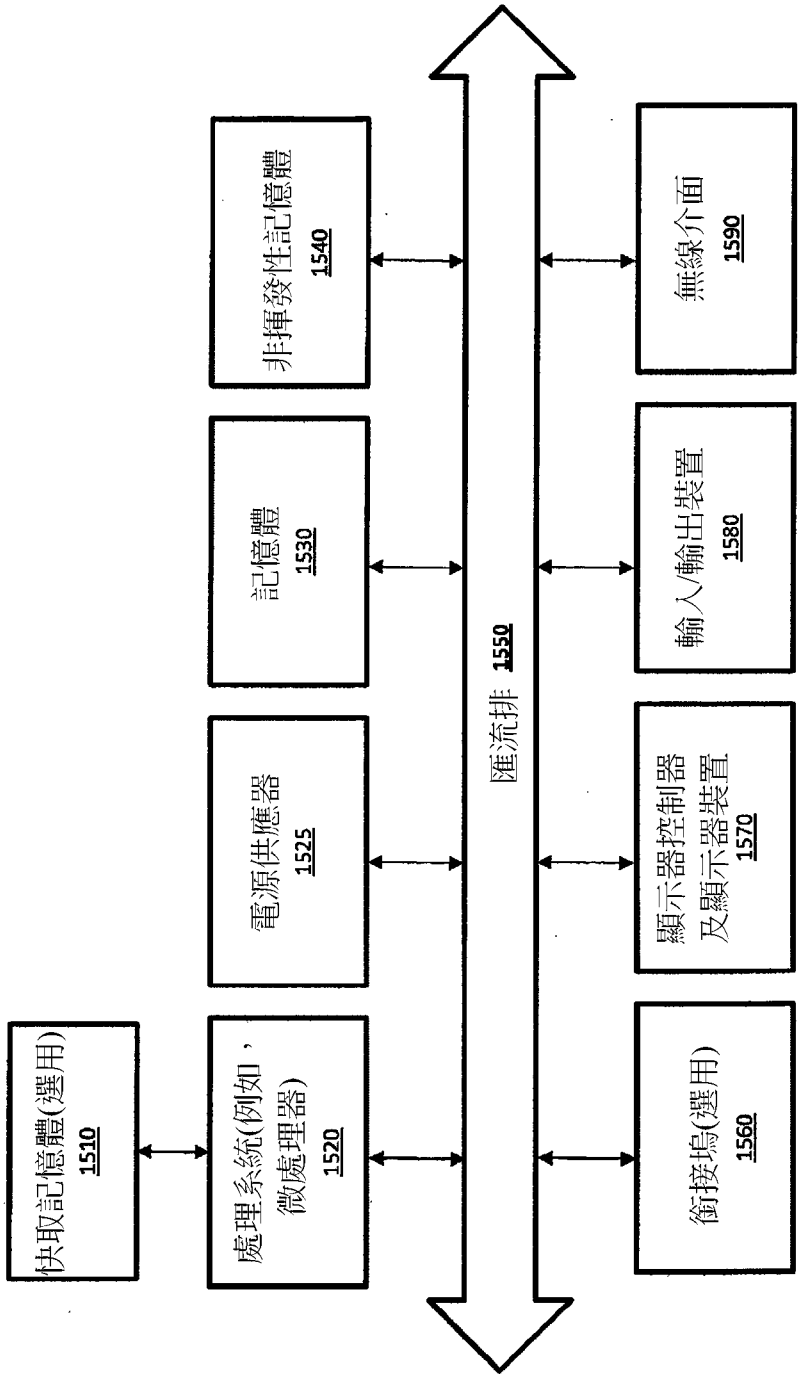
【圖 12】


網站/安全事務伺服器 130
瀏覽器 104
使用者
安全事務外掛程式 105
安全事務服務 101
1301
產生含有對用戶端裝置資訊之查詢之一通知
1302
發送對用戶端資訊之查詢
1303
判定隱私類別；識別資訊以提供至伺服器
1304
發送基於隱私類別所選擇之使用者/用戶端資訊
1305
使用用戶端資訊來啟用與用戶端之安全事務

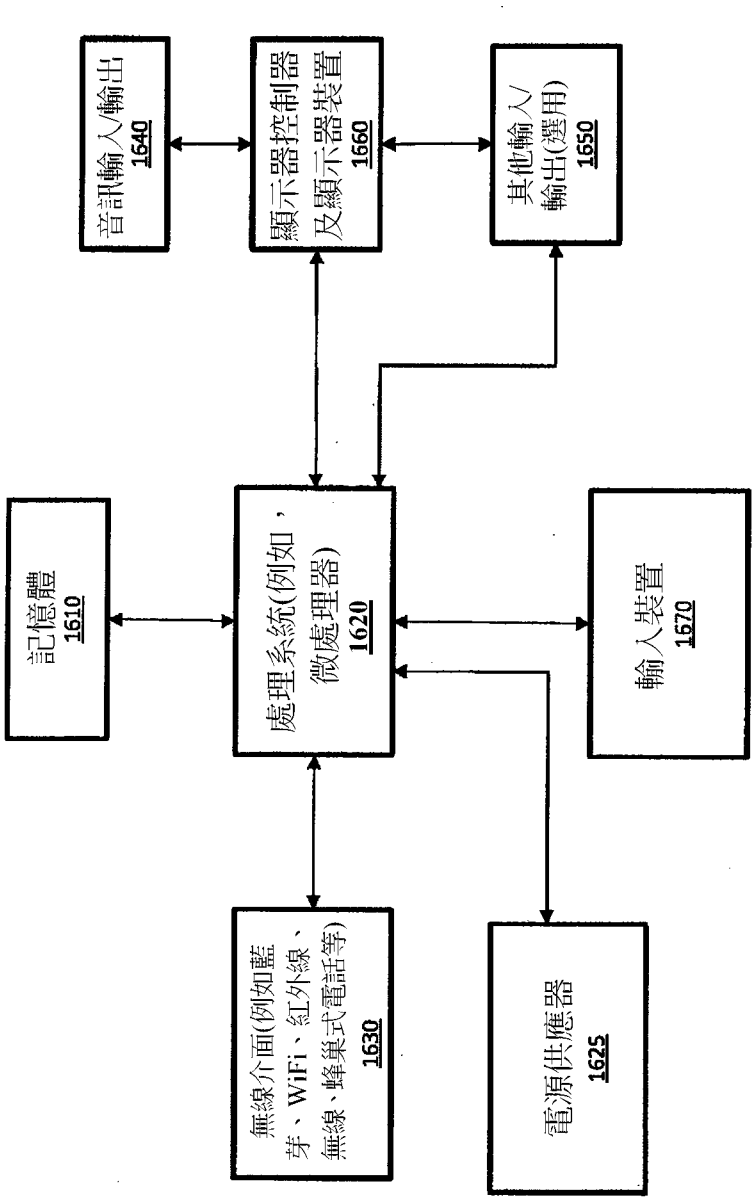
【圖 13】


安全企業或網頁目的地
130
網站或服務
1401
遞交用於
認證之事務
安全事務伺服器
1402
認證
1404
簽章處理
1403
安全事務資料庫
120
伺服器起始事務
•隨機詢問
•事務細節
•簽章{密鑰、事務
細節+隨機詢問}
•隨機詢問
•事務細節
•認證資料
•簽章
用戶端 100

【圖 14】


快取記憶體(選用)
1510
處理系統(例如，微處理器)
1520
電源供應器
1525
記憶體
1530
非揮發性記憶體
1540
匯流排 1550
衛接塢(選用)
1560
顯示器控制器及顯示器裝置
1570
輸入/輸出裝置
1580
無線介面
1590

【圖 15】


音訊輸入/輸出
1640
顯示器控制器及顯示器裝置
1660
其他輸入/輸出(選用)
1650
記憶體
1610
處理系統(例如，微處理器)
1620
輸入裝置
1670
無線介面(例如藍芽、WiFi、紅外線、無線、蜂巢式電話等)
1630
電源供應器
1625

【圖 16】

【發明說明書】

【中文發明名稱】

判定認證能力之查詢系統、方法及非暫態機器可讀媒體

【英文發明名稱】

QUERY SYSTEM, METHOD AND NON-TRANSITORY MACHINE-READABLE MEDIUM TO DETERMINE AUTHENTICATION CAPABILITIES

【技術領域】

本發明一般而言係關於資料處理系統之領域。更特定而言，本發明係關於一種用於判定認證能力之查詢系統及方法。

【先前技術】

現有系統已經設計以用於使用生物識別感測器經由一網路提供安全使用者認證。特定而言，由快速識別線上(FIDO)聯盟開發之一線上安全事務外掛程式(OSTP)協定實現強認證(例如，防身分識別盜竊及網路釣魚之保護)、安全事務(例如，防「瀏覽器中之惡意軟體」及「中間人」對事務之攻擊之保護)及用戶端認證符記(例如，指紋讀取器、面部辨識裝置、智慧卡、可信賴平台模組等)之登記/管理。可(舉例而言)在第2011/0082801號美國專利申請案(「801申請案」)及標題為OSTP Framework之文件(2011年3月23日)中找到現有OSTP協定之細節，該等申請案及文件兩者皆闡述用於一網路上之使用者註冊及認證之一框架。

【發明內容】

【圖式簡單說明】

可連同以下圖式一起自以下詳細說明獲得對本發明之一更好理

解，其中：

圖1A至**圖1B**圖解說明一安全認證系統架構之兩項不同實施例。

圖2係展示可如何發現一用戶端裝置上之認證裝置之一事務圖。

圖3係展示一使用者可如何在認證裝置處登記之一事務圖。

圖4係展示可如何將密鑰註冊至認證裝置中之一事務圖。

圖5係展示可如何在一認證框架內實施使用者認證之一事務圖。

圖6係展示可如何驗證一事務之細節之一事務圖。

圖7圖解說明根據本發明之一項實施例實施之一查詢原則過濾器。

圖8係展示如何在本發明之一項實施例中實施具有查詢原則之一註冊操作之一事務圖。

圖9圖解說明用於實施多個認證裝置處理之一架構之一項實施例。

圖10A至**圖10C**圖解說明用於多個認證裝置處理之本發明之三項實施例。

圖11A至**圖11B**圖解說明用於偵測及迴應於一隨機詢問逾期之一事務圖。

圖12圖解說明根據本發明之一項實施例之用於實施隱私類別之一架構。

圖13係根據本發明之一項實施例之用於實施隱私類別之一事務圖。

圖14圖解說明用於使用簽章來認證之一架構之一項實施例及一事務。

圖15至**圖16**圖解說明用於執行本發明之實施例之一電腦系統之例示性實施例。

【實施方式】

下文闡述用於在一用戶端伺服器環境中智慧地實施一認證框架之一設備、方法及機器可讀媒體之實施例。貫穿說明，出於闡釋之目的，陳述眾多特定細節以便提供對本發明之一透徹理解。然而，熟習此項技術者將明瞭，可在無此等特定細節中之某些細節之情況下實踐本發明。在其他例項中，眾所周知之結構及裝置未展示或以一方塊圖形式展示以避免模糊本發明之基本原理。

下文所論述之本發明之實施例涉及諸如生物識別裝置之具有認證能力之用戶端裝置。此等裝置有時在本文中稱為「符記」。可使用各種不同生物識別裝置，包含(但不限於)指紋感測器、語音辨識硬體/軟體(例如，用於辨識一使用者之語音之一麥克風及相關聯之軟體)、面部辨識硬體/軟體(例如，用於辨識一使用者之臉部之一相機及相關聯之軟體)及光學辨識能力(例如，用於掃描一使用者之視網膜之一光學掃描器及相關聯之軟體)。該等認證能力亦可包含諸如一可信賴平台模組(TPM)及智慧卡之非生物識別裝置。

下文所闡述之本發明之實施例提供優於現有認證技術之各種改良。舉例而言，與需要一用戶端經由一網路傳遞一所有其認證能力(例如，所有其認證符記/裝置)窮盡性清單之當前技術相比，本發明之一項實施例實施其中一安全事務伺服器最初將指示由伺服器接受之認證能力之一伺服器原則傳輸至用戶端之一查詢原則。用戶端接著分析伺服器原則以識別一子組認證能力，藉此減小對用戶端之隱私影響。

在另一實施例中，採用多個可組態隱私等級保護。隱私類別經預定義且可由終端使用者選擇及/或修改。在本發明之一項實施例中，基於可使用所請求資訊識別一用戶端之概率定義隱私類別。在相對較高隱私等級(具有一相對較低隱私影響)下，關於用戶端裝置之相對較少資訊經洩漏以執行本文中所闡述之認證技術。

本發明之另一實施例同時提供多個裝置之佈建或認證，藉此改良效率。舉例而言，代替一次請求對一單個認證裝置之註冊或認證，可自伺服器發送一認證裝置清單。對稱及/或不對稱密鑰接著在本機執行於用戶端上之一個操作或系列順序操作中佈建至多個符記/裝置中。對於認證，數個符記/裝置可同時經選擇以用於一既定事務。

本發明之另一實施例改良處理及管理伺服器詢問之效率。當今，在一伺服器將一隨機詢問(例如，一密碼編譯臨時用法)發送至用戶端之後，若用戶端在一規定逾期時間內未回應，則臨時用法不再有效且用戶端將回應於一後續認證嘗試接收一錯誤。舉例而言，若使用者使用戶端暫停移動至一新位置(例如，關閉一膝上型電腦上之蓋)且接著嘗試認證，則認證嘗試將被拒絕。在本發明之一項實施例中，用戶端偵測到隨機詢問已期滿且自伺服器自動及透通地請求一新詢問。接著伺服器產生一新詢問且將其傳輸至其中其可用於認證之用戶端。終端使用者體驗經改良，此乃因使用者不接收一錯誤或一認證請求之拒絕。

本發明之另一實施例採用在一安全事務伺服器上之事務簽章以使得不需要將事務狀態維持在該伺服器上來維持與用戶端之當前工作階段。由伺服器簽章之事務內容(諸如事務文字)發送至用戶端，當用

戶端做出回應時，其將具有簽章之事務內容發送回。伺服器不需要儲存事務狀態，此乃因其可驗證由用戶端接收之經簽章事務回應係藉由驗證簽章有效的。

儘管上文闡述為單獨實施例，但所有上文技術可以各種方式一起組合於一單個綜合認證系統內。因此，本發明之一既定實施例可與本文中所闡述之一或多個其他實施例組合以用於在一安全網路環境中改良用戶端及使用者認證。

例示性系統架構

圖1A至**圖1B**圖解說明包括用於認證一使用者之用戶端側及伺服器側組件之一系統架構之兩項實施例。**圖1A**中所展示之實施例使用用於與一網站通信之一基於瀏覽器外掛程式架構而**圖1B**中所展示之實施例不需要一瀏覽器。可在此等系統架構中之任一者上實施本文中所闡述之各種技術，諸如在認證裝置處登記一使用者、在一安全伺服器處註冊認證裝置及認證一使用者。因此，儘管**圖1A**中所展示之架構用以表明下文所闡述之實施例中之數項實施例之操作，但相同基本原理可容易地實施於**圖1B**中所展示之系統上(例如，藉由移除作為用於伺服器130與用戶端上之安全事務服務101之間的通信之中介機構之瀏覽器外掛程式105)。

首先翻至**圖1A**，所圖解說明之實施例包含裝備有用於登記及認證一終端使用者之一或多個認證裝置110至112 (有時在此項技術中稱為認證「符記」)之一用戶端100。如上文所提及，認證裝置110至112可包含：生物識別裝置，諸如指紋感測器、語音辨識硬體/軟體(例如，用於辨識一使用者之語音之一麥克風及相關聯之軟體)、面部辨

識硬體/軟體(例如，用於辨識一使用者之臉部之一相機及相關聯之軟體)及光學辨識能力(例如，用於掃描一使用者之視網膜之一光學掃描器及相關聯之軟體)；及非生物識別裝置，諸如一可信賴平台模組(TPM)及智慧卡。

認證裝置110至112透過由一安全事務服務101曝露之一介面102(例如，一應用程式程式化介面或API)以通信方式耦合至用戶端。安全事務服務101係用於與一或多個安全事務伺服器132至133經由一網路通信及用於與在一網頁瀏覽器104之內容脈絡內執行之一安全事務外掛程式105介接之一安全應用程式。如所圖解說明，介面102亦可提供至用戶端100上之一安全儲存裝置120之安全存取，該安全儲存裝置儲存與認證裝置110至112中之每一者相關之資訊，諸如一裝置識別碼、使用者識別碼、使用者登記資料(例如，經掃描指紋或其他生物識別資料)及用以執行本文中所闡述之安全認證技術之密鑰。舉例而言，如下文詳細論述，一唯一密鑰可儲存至認證裝置中之每一者中且在經由諸如網際網路之一網路傳遞至伺服器130時使用。

如下文所論述，特定類型之網路事務由安全事務外掛程式105支援，諸如與網站131或其他伺服器之HTTP或HTTPS事務。在一項實施例中，安全事務外掛程式回應於藉由安全企業或網頁目的地130 (有時在下文簡稱為「伺服器130」)內之網頁伺服器131插入至一網頁之HTML碼中之特定HTML標籤起始。回應於偵測到此一標籤，安全事務外掛程式105可將事務轉發至安全事務服務101以供處理。另外，針對特定類型之事務(例如，諸如安全密鑰交換)，安全事務服務101可打開與內部部署事務伺服器132 (亦即，與網站共同定位)或與一外部

部署事務伺服器133之一直接通信通道。

安全事務伺服器132至133耦合至用於儲存使用者資料、認證裝置資料、密鑰及支援下文所闡述之安全認證事務所需之其他安全資訊之一安全事務資料庫120。然而，應注意，本發明之基本原理不需要**圖1A**中所展示之安全企業或網頁目的地130內之邏輯組件之分離。舉例而言，網站131及安全事務伺服器132至133可實施於一單個實體伺服器或單獨實體伺服器內。此外，網站131及事務伺服器132至133可實施於執行於一或多個伺服器上之一積體軟體模組內以用於執行下文所闡述功能。

如上文所提及，本發明之基本原理不限於**圖1A**中所展示之一基於瀏覽器架構。**圖1B**圖解說明其中一獨立應用程式154利用由安全事務服務101提供之功能性來經由一網路認證一使用者之一替代實施方案。在一項實施例中，應用程式154經設計以建立與依賴於安全事務伺服器132至133之一或多個網路服務151之通信工作階段以用於執行下文詳細闡述之使用者/用戶端認證技術。

在**圖1A**至**圖1B**中所展示之實施例中之任一者中，安全事務伺服器132至133可產生密鑰，接著該等密鑰安全地傳輸至安全事務服務101且儲存至認證裝置中於安全儲存裝置120內。另外，安全事務伺服器132至133管理在伺服器側上之安全事務資料庫120。

裝置發現、登記、註冊及認證之一概述

圖2至**圖6**中展示用於執行認證裝置發現、登記、註冊及認證之一例示性系列事務。在上文所提及之OSTP協定(參見OSTP框架(2011年3月23日)來看額外細節，該OSTP框架以引用方式併入本文中)中已

採用此等事務之某些態樣。對此等事務之基本操作之一理解將提供其中可實施本發明之實施例之一內容脈絡。

下文所闡述之操作包含認證裝置之偵測(**圖2**)；使用者在認證裝置處之登記(**圖3**)；認證裝置之註冊(**圖4**)；在經註冊認證裝置處之使用者認證(**圖5**)；及在認證之後之安全事務之實施方案(**圖6**)。

圖2圖解說明用於偵測用戶端機器上之認證裝置之一系列事務。在裝置偵測成功地完成之後，伺服器130處理關於附接至用戶端之認證裝置之窮盡性資訊且將能夠評估哪個(些)裝置係最適合於與經增強安全性基礎結構一起使用。僅伺服器130過濾認證裝置清單。使用者將提供有此清單且可選擇認證裝置中之一者(或組合)來用於進一步認證及安全事務之實施方案。

在操作中，使用者用使用者名稱及密碼在瀏覽器中認證且登入至網站。此係唯一一次將需要使用者提供一使用者名稱及密碼。伺服器130判定使用者當前未使用經增強安全性(例如，藉由查詢安全事務資料庫120)且將一建議提供至使用者以改變為經增強安全性。

在一項實施例中，伺服器130包含安全事務外掛程式105偵測到之一HTML頁中之一「對裝置之查詢」標籤。回應於偵測到標籤，安全事務外掛程式105將請求重路由至安全事務服務101，該安全事務服務接著準備關於附接至系統之所有認證裝置之包含裝置之安全性特性之窮盡性資訊。在一項實施例中，資訊在使用一預先規定之資料結構描述傳輸之前以一XML格式經封裝。

安全事務外掛程式105自安全事務服務101接收此資訊且在一項實施例中將資訊經由一經註冊回撥遞送至網頁之JavaScript。其接著

選擇如何顯示瀏覽器104中之資訊。由網站過濾之清單可展示給使用者且使用者可選擇認證裝置中之一者或一組合。

圖3圖解說明用以在認證裝置處登記使用者之一系列事務。在一項實施例中，登記係使用由本文中所闡述之本發明之實施例提供之經增強安全性之一必備條件。登記涉及採取讀取使用者(例如，一指紋、語音樣本等)之一生物識別以使得相同認證裝置可在一後續事務期間用以認證使用者。登記操作可在不與伺服器130互動之情況下僅在用戶端上完成。針對登記提供之使用者介面可顯示於瀏覽器擴充套件中或可顯示於一單獨應用程式或行動裝置應用程式中。

只要偵測到裝置，即可起始登記操作。使用者可選擇使用所發現裝置中之一者或一群組以用於經增強安全性。在操作中，使用者可自瀏覽器、應用程式或行動裝置應用程式中之所顯示裝置清單選擇一裝置。對於**圖3**中所圖解說明之基於瀏覽器實施方案，安全事務外掛程式105顯示一裝置特定登記圖形使用者介面(GUI)。安全事務外掛程式105將裝置識別符及一登記請求傳輸至安全事務服務101且等待完成。若使用者已在用戶端上之一認證裝置處登記，則使用者可僅需要驗證其身分識別(亦即，其將不需要再次登記)。若使用者當前未登記，則安全事務服務101藉由啟動實體認證裝置(例如，經由裝置介面102)開始登記程序。使用者接著與安全事務外掛程式105 GUI互動且遵循規定登記步驟(例如，撥動一手指、對一麥克風講話、抓拍一圖片等)。一旦完成，使用者便將在認證裝置處登記。顯著地，一旦一使用者在一裝置處登記，其便可使用此登記來在如本文中所闡述之任何網站或網路服務處註冊或認證。

圖4圖解說明用於認證裝置之註冊之一系列事務。在註冊期間，一密鑰在認證裝置與安全事務伺服器132至133中之一者之間共用。密鑰儲存於用戶端100之安全儲存裝置120及由安全事務伺服器132至133使用之安全事務資料庫120內。在一項實施例中，密鑰係由安全事務伺服器132至133中之一者產生之一對稱密鑰。然而，在下文所論述之另一實施例中，可使用不對稱密鑰。在此實施例中，公共密鑰可由安全事務伺服器132至133儲存且一第二相關私密密鑰可儲存於用戶端上之安全儲存裝置120中。此外，在一項實施例(下文亦論述)中，密鑰可產生於用戶端100上(例如，藉由認證裝置或認證裝置介面而非安全事務伺服器132至133)。

諸如動態對稱密鑰佈建協定(DSKPP)之一安全密鑰佈建協定可用以與用戶端經由一安全通信通道共用密鑰(參見例如請求註解(RFC)6063)。然而，本發明之基本原理不限於任何特定密鑰佈建協定。

翻至**圖4**中所展示之特定細節，一旦使用者登記或使用者認證完成，伺服器130便產生在裝置註冊期間必須由用戶端呈現之一隨機產生詢問(例如，一密碼編譯臨時用法)。隨機詢問可在一有限時段內有效。安全事務外掛程式偵測到隨機詢問且將其轉發至安全事務服務101。作為回應，安全事務服務起始與伺服器130之一帶外（out-of-band）工作階段(例如，一帶外事務)且使用密鑰佈建協定與伺服器130通信。伺服器130用使用者名稱定位使用者、確證隨機詢問、確證裝置之認證碼(若發送一個認證碼)且在安全事務資料庫120中為使用者形成一新項目。其亦可產生密鑰、將密鑰寫入至資料庫120且使用密鑰佈建協定將密鑰發送回至安全事務服務101。一旦完成，認證裝

置及伺服器130便共用相同密鑰(若使用一對稱密鑰)或不同密鑰(若使用不對稱密鑰)。

圖5圖解說明用於使用者在經註冊認證裝置處認證之一系列事務。一旦裝置註冊完成，伺服器130便將接受由本機認證裝置產生之一符記作為一有效認證符記。

翻至**圖5**中所展示之特定細節，其展示一基於瀏覽器實施方案，使用者在瀏覽器104中鍵入伺服器130之統一資源定位符(URL)。在使用一獨立應用程式或行動裝置應用程式(而非一瀏覽器)之一實施方案中，使用者可鍵入一網路服務之一網路位址或應用程式或應用程式可自動嘗試連接至網路位址處之網路服務。

對於一基於瀏覽器實施方案，網站在HTML頁中嵌入對所註冊裝置之一查詢。除在一HTML頁中嵌入查詢之外，此可以諸多方式完成，諸如透過JavaScript或使用HTTP標頭。安全事務外掛程式105接收URL且將其發送至安全事務服務101，該安全事務服務搜尋瀏覽安全儲存裝置120 (其如所論述包含認證裝置之一資料庫及使用者資訊)且判定此URL內是否存在登記之一使用者。若如此，則安全事務服務101將與此URL相關聯之一佈建裝置清單發送至安全事務外掛程式105。安全事務外掛程式接著呼叫經註冊JavaScript API且將此資訊遞送至伺服器130 (例如，網站)。伺服器130自所發送裝置清單選擇適當裝置、產生一隨機詢問且將裝置資訊及引數發送回至用戶端。網站顯示對應使用者介面且自使用者請求認證。使用者接著提供所請求認證措施(例如，跨越指紋讀取器撥動一手指、講話以供語音辨識等)。安全事務服務101識別使用者(此步驟可針對不支援儲存使用者之裝置跳

過)、自資料庫獲得使用者名稱、使用密鑰產生一認證符記且經由安全事務外掛程式將此資訊發送至網站。伺服器130自安全事務資料庫120識別使用者且藉由在伺服器130上產生相同符記(例如，使用其密鑰之複本)驗證符記。一旦經驗證，認證程序便完成。

圖6圖解說明遵循用於一基於瀏覽器實施方案之認證之一安全事務。安全事務經設計以為特定類型之事務(例如，財務事務)提供更強安全性。在所圖解說明之實施例中，使用者在認可事務之前確認每一事務。使用所圖解說明之技術，使用者確認其究竟希望認可何種內容及究竟認可顯示於GUI中之其看見之何種內容。換言之，此實施例確保事務文字不可由一「中間人」修改以認可使用者未確認之一事務。

在一項實施例中，安全事務外掛程式105在瀏覽器內容脈絡中顯示一窗601以展示事務細節。安全事務伺服器101週期性地(例如，以一隨機時間間隔)驗證展示於窗中之文字不被任何人篡改。

以下實例將有助於突出此實施例之操作。一使用者自一商家地址選擇購買之物項且選擇「結帳」。商家地址將事務發送至具有實施本文中所闡述之本發明之實施例中之一或多者之一安全事務伺服器132至133之一服務提供商(例如，PayPal)。商家地址認證使用者且完成事務。

安全事務伺服器132至133接收事務細節(TD)且將一「安全事務」請求放入一HTML頁中且發送至用戶端100。安全事務請求包含事務細節及一隨機詢問(例如，一隨機臨時用法)。安全事務外掛程式105偵測到對事務確認訊息之請求且將所有資料轉發至安全事務服務101。在不使用一瀏覽器或外掛程式之一實施例中，資訊可自安全事

務伺服器直接發送至用戶端100上之安全事務服務。

對於一基於瀏覽器實施方案，安全事務外掛程式105將具有事務細節之一窗601顯示給使用者(在一瀏覽器內容脈絡中)且邀請使用者提供用以確認事務之認證。在不使用一瀏覽器或外掛程式之一實施例中，安全事務服務101或應用程式154可顯示窗601。安全事務服務101開始一計時器且驗證被顯示給使用者之窗601之內容。可隨機選擇驗證之時段。安全事務服務101確保使用者在窗601中看見有效事務細節。若其偵測到內容已經篡改，則其防止產生確認符記。

在使用者提供有效認證(例如，在指紋感測器上撥動一手指)之後，裝置識別使用者且藉助事務細節及隨機詢問產生一符記(密碼編譯簽章) (亦即，經由事務細節及臨時用法計算符記)。此允許安全事務伺服器132至133確保，事務細節尚未在伺服器與用戶端之間經修改。安全事務服務101將所產生符記及使用者名稱發送至安全事務外掛程式105，該安全事務外掛程式將符記轉發至安全事務伺服器132至133。安全事務伺服器132至133用使用者名稱及驗證符記識別使用者。若驗證成功，則將一確認訊息發送至用戶端且處理事務。

用於一安全查詢之系統及方法

用以判定用戶端認證能力之原則

如所提及，本發明之一項實施例實施其中一安全事務伺服器將指示由伺服器接受之認證能力之一伺服器原則傳輸至用戶端之一查詢原則。用戶端接著分析伺服器原則以識別其支援之及/或使用者已表達一意願來使用之一子組認證能力。用戶端接著使用匹配所提供原則之子組認證符記來註冊及/或認證使用者。因此，存在對用戶端之隱

私之一較低影響，此乃因不需要用戶端傳輸關於其認證能力(例如，所有其認證裝置)之窮盡性資訊或可用以唯一地識別用戶端之其他資訊。

藉由實例而非限制方式，用戶端可包含眾多認證能力，諸如一指紋感測器、語音辨識能力、面部辨識能力、眼睛/光學辨識能力、一可信賴平台模組(TPM)及智慧卡(僅舉幾例)。然而，出於隱私原因，使用者可能不希望對一請求伺服器洩漏所有其能力之細節。因此，使用本文中所闡述之技術，安全事務伺服器可將指示其支援(舉例而言)指紋、光學或智慧卡認證之一伺服器原則傳輸至用戶端。用戶端可接著比較伺服器原則與其自身認證能力且選擇可用認證選項中之一或多者。

圖7圖解說明用於實施此等技術之一用戶端伺服器架構之一項實施例。如所圖解說明，實施於用戶端100上之安全事務服務101包含用於分析由伺服器130提供之原則且識別將用於註冊及/或認證之一子組認證能力之一原則過濾器701。在一項實施例中，原則過濾器701實施為執行於安全事務服務101之內容脈絡內之一軟體模組。然而，應注意，原則過濾器701可以任何方式實施而仍遵守本發明之基本原理且可包含軟體、硬體、韌體或其任何組合。

圖7中所展示之特定實施方案包含用於使用先前所論述之技術建立與安全企業或網頁目的地130 (有時簡稱為「伺服器130」)之通信之一安全事務外掛程式105。舉例而言，安全事務外掛程式可識別由一網頁伺服器131插入至HTML碼中之一特定HTML標籤。因此，在此實施例中，伺服器原則提供至安全事務外掛程式105，該安全事務外掛

程式將其轉發至實施原則過濾器701之安全事務服務101。

原則過濾器701可藉由自用戶端之安全儲存區域720讀取能力判定用戶端認證能力。如先前所論述，安全儲存裝置720可包括所有用戶端之認證能力(例如，所有認證裝置之識別碼)之一儲存庫。若使用者已在其認證裝置處登記使用者，則使用者之登記資料儲存於安全儲存裝置720內。若用戶端已在一伺服器130處註冊一認證裝置，則安全儲存裝置亦可儲存與每一認證裝置相關聯之一經加密秘密密鑰。

使用自安全儲存裝置720提取之認證資料及由伺服器提供之原則，原則過濾器701可接著識別將使用之一子組認證能力。取決於組態，原則過濾器701可識別由用戶端及伺服器兩者支援之一認證能力完整清單或可識別一子組完整清單。舉例而言，若伺服器支援認證能力A、B、C、D及E且用戶端具有認證能力A、B、C、F及G，則原則過濾器701可給伺服器識別整個子組共同認證能力：A、B及C。另一選擇係，若期望一較高隱私等級(如由**圖7**中之使用者偏好730指示)，則可給伺服器識別一更有限子組認證能力。舉例而言，使用者可指示，應給伺服器識別僅一單個共同認證能力(例如，A、B或C中之一者)。在一項實施例中，使用者可針對用戶端100之所有認證能力建立一優先化方案且原則過濾器可選擇伺服器及用戶端兩者所共有之最高優先權認證能力(或一優先化組*N個*認證能力)。

取決於何種操作已由伺服器130起始(註冊或認證)，安全事務服務130對該組經過濾子認證裝置(110至112)執行彼操作且將操作回應經由安全事務外掛程式105發送回至伺服器130，如**圖7**中所展示。另一選擇係，在不依賴於一網頁瀏覽器之一外掛程式105組件之一實施

例中，資訊可自安全事務服務101直接遞送至伺服器130。

圖8圖解說明展示具有查詢原則事務之一例示性系列註冊之額外細節之一事務圖。在所圖解說明之實施例中，使用者先前尚未在伺服器130處註冊裝置。因此，在801處，作為一初始一次性認證步驟，使用者可鍵入一使用者名稱及密碼，該使用者名稱及密碼在802處經由用戶端瀏覽器104轉發至伺服器130。然而，應注意，遵守本發明之基本原理不需要一使用者名稱及密碼。

由於使用者先前尚未以經增強安全性註冊(在803處判定)，因此伺服器130在804處將其伺服器原則傳輸至用戶端。如所提及，伺服器原則可包含由伺服器130支援之認證能力之一指示。在所圖解說明之實例中，經由事務806將伺服器原則遞送至安全事務服務101。

在事務807處，安全事務服務101比較伺服器原則與用戶端之能力(及諸如如上文所闡述之裝置優先權方案及/或使用者偏好之潛在地其他資訊)以得出一經過濾之認證能力清單。經過濾之裝置(102)清單接著產生密鑰(808及809)且接著將此等密鑰之公共部分提供至安全事務服務101，該安全事務服務繼而將此等部分作為註冊回應發送回至伺服器130(810)。伺服器證實認證裝置且將公共密鑰儲存於安全事務資料庫中(811)。此處採用之符記證實係在註冊期間確證認證裝置身分識別之程序。其允許伺服器以密碼編譯方式確保由用戶端報告之裝置實際上係其聲稱之裝置。

另一選擇係或另外，在807處，使用者可提供有一機會來審閱清單及/或選擇將與此特定伺服器130一起使用之特定認證能力。舉例而言，經過濾清單可指示與一指紋掃描、面部辨識及/或語音辨識一起

使用認證之選項。使用者可接著在於伺服器130處認證時選擇使用此等選項中之一或多者。

上文所闡述之用於在一用戶端處過濾一伺服器原則之技術可實施於上文所闡述之系列事務之各種不同階段處(例如，在裝置發現、裝置註冊、裝置佈建、使用者認證等期間)。亦即，本發明之基本原理不限於**圖8**中陳述之特定組事務及特定事務排序。

此外，如先前所提及，遵守本發明之基本原理不需要一瀏覽器外掛程式架構。對於涉及一瀏覽器或瀏覽器外掛程式(例如，諸如一獨立應用程式或行動裝置應用程式)之一架構，**圖8**中所展示之事務圖(及本文中所揭示之其餘事務圖)可經簡化以使得瀏覽器104經移除且安全事務服務101與伺服器130直接通信。

用於在多個認證裝置處有效地登記、註冊及認證之系統及方法

本發明之一項實施例能夠同時登記、註冊及認證多個裝置，藉此改良效率及使用者體驗。舉例而言，代替一次請求對一單個裝置之註冊及認證，可將一裝置清單發送至用戶端。對稱或不對稱密鑰可接著在本機執行於用戶端上之一個操作中或系列順序操作中註冊至多個裝置中。對於認證，數個符記/裝置可同時經選擇以用於一既定事務。

圖9圖解說明用於實施此等技術之一用戶端伺服器架構之一項實施例。如所圖解說明，實施於用戶端100上之安全事務服務101包含用於在不需要在每一裝置經登記/註冊時與伺服器130連續來回通信之情況下一次執行諸如多個裝置之登記及註冊之規定操作之多裝置處理邏輯901。類似地，伺服器130包含用於發佈引導至多個認證裝置之命令

之多裝置處理邏輯。在一項實施例中，多裝置處理邏輯901實施為執行於安全事務服務101之內容脈絡內之一軟體模組。然而，應注意，多裝置處理邏輯901可以任何方式實施而仍遵守本發明之基本原理且可包含軟體、硬體或韌體組件或其任何組合。

如在上文所闡述之實施例中，**圖9**中所展示之特定實施方案包含用於建立與伺服器130 (其如所論述可包含一網站伺服器131及安全事務伺服器132至133)之通信之安全事務外掛程式105。因此，伺服器130與安全事務服務101經由安全事務外掛程式105通信。然而，如所提及，遵守本發明之基本原理不需要一基於瀏覽器外掛程式架構。

伺服器130上之多裝置處理邏輯902可傳遞將由對多個認證裝置110至112執行操作之用戶端100上之多裝置處理邏輯901執行之命令。藉由實例之方式，多裝置處理邏輯902可產生將在N個認證裝置中之每一者處註冊且接著連同用以註冊N個裝置之一命令一起安全地傳輸至多裝置處理邏輯901之N個密鑰。多裝置處理邏輯901可接著在不與伺服器進一步互動之情況下同時或以一系列順序操作執行對所有N個裝置(例如，對認證裝置110至112)之註冊。一單個回應可接著發送至伺服器130以指示所有N個裝置之完成註冊。

一系列例示性多裝置事務圖解說明於**圖10A**至**圖10C**中。**圖10A**圖解說明可在無與伺服器130之任何互動之情況下執行之一多裝置登記程序(例如，可在用戶端上之安全事務服務101之控制下執行在認證裝置處登記使用者)。在一替代實施例中，伺服器130可將一請求傳輸至用戶端(未展示)以在N個裝置處登記使用者。**圖10B**至**圖10C**圖解說明用於在伺服器130處註冊多個裝置之兩項不同實施例。

翻至**圖10A**中之登記程序，在1001處，使用者表達在用戶端上之N個認證裝置(表示所有或一子組可用認證裝置)處登記之一願望。作為回應，在1002處呼叫安全事務外掛程式且在1003處產生一裝置特定圖形使用者介面(GUI)以使使用者通過程序或在認證裝置#1處登記。在登記程序期間，使用者如所指示與安全事務外掛程式互動(例如，藉由將一手指定位於一指紋感測器上方、對一麥克風講話、用相機等抓拍一圖片)。在一項實施例中，對N個裝置中之每一者執行登記直至在1004處完成對第N個裝置之登記為止。一不同裝置特定描述性語言及/或使用者介面可呈現給使用者以在每一個別認證裝置處登記使用者。如先前所論述，在使用者在每一裝置處登記時，使用者登記資料可儲存於用戶端100上之安全儲存裝置720內且使得可僅透過安全事務服務101來存取。一旦完成對所有N個裝置之登記，便可經由事務1004至1005將一通知發送至伺服器130。

無論如何執行登記，一旦完成，**圖10B**中所展示之事務圖便可用以在伺服器130處註冊N個裝置。在1010處伺服器130產生一使用者特定隨機詢問，如先前所闡述，該使用者特定隨機詢問可僅在一有限時間窗內有效且可包括諸如一密碼編譯臨時用法之一隨機產生碼。在1011處，隨機詢問連同一命令一起傳輸以在伺服器130處註冊N個認證裝置。在1012處，安全事務服務101形成與伺服器130之一安全連接且將用於N個裝置之識別資料連同隨機詢問一起傳輸。在一項實施例中，安全連接係一HTTPS連接。然而，本發明之基本原理不限於任何特定安全連接類型。

在1013處，伺服器130證實N個裝置、產生用於N個裝置中之每一

者之一密鑰且將N個密鑰經由安全連接發送回至安全事務服務。在一項實施例中，動態對稱密鑰佈建協定(DSKPP)用以與用戶端經由安全連接交換密鑰。然而，本發明之基本原理不限於任何特定密鑰佈建技術。另一選擇係，在不依賴於DSKPP協定之一實施例中，密鑰可產生於每一認證裝置中且接著傳輸至伺服器130。

在1014至1015處，安全事務服務之多裝置處理邏輯將N個密鑰中之每一者註冊至N個裝置中之每一者中。如先前所闡述，每一密鑰可經儲存且與用戶端上之安全儲存裝置720內之其各別裝置相關聯。一旦完成對每一認證裝置之註冊，便在1016處經由安全連接將一通知發送至伺服器。

在一項實施例中，註冊至每一認證裝置中之密鑰係對稱密鑰。因此，每一密鑰之一相同複本儲存於用戶端上之安全儲存裝置720及伺服器130上之安全事務資料庫120中。在一替代實施方案中，可產生不對稱密鑰對，其中密鑰中之一者作為一公共密鑰維持於伺服器上之安全事務資料庫120中及作為私密密鑰儲存於用戶端之安全儲存裝置720中。然而，應注意，本發明之基本原理不限於任何特定類型之加密密鑰。

一替代實施方案圖解說明於**圖10C**中，其中密鑰產生於用戶端而非伺服器130上。在此實施方案中，在於1011處接收對用隨機詢問註冊裝置之請求之後，安全事務服務101之多裝置處理邏輯在1120處產生用於N個裝置中之每一者之N個密鑰。一旦經產生，密鑰在1013至1014處在N個裝置中之每一者處註冊且註冊儲存於安全儲存裝置720內，如先前所闡述。一旦所有密鑰已經註冊，安全事務服務101便在

1015處將一通知連同隨機詢問一起提供至伺服器(以驗證用戶端之身分識別)。伺服器130可接著將註冊儲存於安全事務資料庫120中，如上文所闡述。

用於處理一認證框架內之隨機詢問之系統及方法

本發明之一項實施例改良隨機詢問由伺服器產生及處理之方式。在一項實施例中，隨機詢問包括諸如一密碼編譯臨時用法之一隨機產生碼。在當前系統中，在一伺服器將一隨機詢問傳輸至用戶端之後，若用戶端不在一規定逾期時間內回應，則隨機詢問不再有效且用戶端將回應於一後續認證嘗試接收一錯誤(例如，使用者將在指紋讀取器上撥動一手指且被拒絕)。

在本發明之一項實施例中，用戶端自動偵測到詢問已期滿且自伺服器透通地請求一新詢問(亦即，在無使用者干預之情況下)。伺服器接著產生一新隨機詢問且將其傳輸至用戶端，用戶端可接著使用其來建立與伺服器之安全通信。終端使用者體驗經改良，此乃因使用者不接收一錯誤或一認證請求之拒絕。

圖11A圖解說明在一註冊程序之內容脈絡內使用之一項此實施例，且**圖11B**圖解說明在一認證程序之內容脈絡內使用之一實施例。然而，應注意，可在除**圖11A**至**圖11B**中所展示之彼等內容脈絡之外的內容脈絡中採用本發明之基本原理。舉例而言，本文中所闡述之技術可與其中一時間敏感碼自一伺服器傳遞至一用戶端之任何程序一起使用。

首先翻至**圖11A**，在1101處，伺服器130產生一隨機詢問及一逾期時間之一指示。在一項實施例中，逾期時間包括在其內認為隨機詢

問有效之一時段。在逾期時間已過去之後，隨機詢問不再由伺服器130認為係有效的。在一項實施例中，逾期時間簡單地規定為隨機詢問將不再有效之一時間點。一旦到達此時間點，隨機詢問便無效。在另一實施例中，藉由使用一當前時間戳記(亦即，隨機詢問由伺服器130產生之時間)及一持續時間規定逾期時間。安全事務服務101可接著藉由將持續時間值與時間戳記相加以計算隨機詢問變為無效時之時間點而計算逾期時間。然而，應注意，本發明之基本原理不限於用於計算逾期時間之任何特定技術。

無論逾期時間如何被規定或計算，在1102處將隨機詢問及逾期指示傳輸至安全事務服務101 (經由所圖解說明之實例中之瀏覽器104及安全事務外掛程式105)。在1103處，安全事務服務101偵測到隨機詢問已逾期且不再基於自伺服器130發送之逾期指示有效。藉由實例之方式，使用者可在完成系列事務之前已關閉其用戶端機器或關閉其筆記本電腦上之蓋。若事務係需要使用者互動之事務，則使用者可能已簡單地避開或忽略顯示於GUI內之一訊息。

在1104處，在偵測到隨機詢問不再有效時，安全事務服務101將對一新隨機詢問之一請求傳輸至伺服器130 (經由所圖解說明之實例中之安全事務外掛程式105及瀏覽器104)。在1105處，伺服器130產生一新隨機詢問及逾期時間之一新指示。在一項實施例中，逾期時間係與在操作1101中相同的或可經修改。舉例而言，伺服器130可增加逾期時間之持續時間以減小與用戶端之資料訊務或減少持續時間以增大由隨機詢問提供之安全性等級。在1106處，將新隨機詢問及逾期指示傳輸至安全事務服務101。

事務之其餘部分如先前所闡述發生。舉例而言，安全事務服務在1107處打開直接至伺服器之一安全連接以便執行裝置註冊及密鑰交換，如上文關於**圖4**、**圖10B**或**圖10C**所論述。在1108處，伺服器130識別使用者(例如，用一使用者名稱或其他ID)、證實認證裝置且產生用於裝置之一密鑰。如所提及，密鑰可係一對稱密鑰或一不對稱密鑰。在1109處，將密鑰經由安全連接傳輸至安全事務服務101且在1110處，安全事務服務101將密鑰註冊至認證裝置中。在1111處，將完成註冊之一通知傳輸至伺服器130。

因此，在**圖11A**中所展示之實施例中，用於裝置註冊之密鑰如在**圖10B**中所展示之實施例中在伺服器130處產生。然而，亦可在其中密鑰由用戶端100上之安全事務服務101產生之一實施例(諸如上文關於**圖10C**所闡述之實施例)中使用本發明之基本原理。

圖11B圖解說明在一認證程序之內容脈絡內實施之本發明之一項實施例。在1151處，使用者將一特定網站URL鍵入至瀏覽器104中且將其引導至包含安全事務伺服器132至133之企業/網頁目的地伺服器130內之網頁伺服器131。在1152處，將一查詢發送回至安全事務服務(經由瀏覽器及外掛程式)以判定在網站之URL處註冊哪個(些)裝置。安全事務服務101查詢用戶端100上之安全儲存裝置720以識別在1153處發送回至伺服器130之一裝置清單。在1154處，伺服器1154選擇一裝置來用於認證、產生一隨機詢問及一逾期指示且在1155處，將此資訊發送回至安全事務服務101。

在1156處，安全事務服務1156自動偵測到在達到逾期時間之結束後隨機詢問旋即不再有效。如上文所提及，可採用各種不同技術以用

於指示及偵測逾期時間之結束(參見**圖11A**及相關聯之文字)。在偵測到隨機詢問之期滿後，在1157處，安全事務服務101旋即透通地(亦即，在無使用者干預之情況下)通知伺服器130且請求一新隨機詢問。作為回應，在1158處，伺服器130產生一新隨機詢問及逾期時間之一新指示。如所提及，新逾期時間可係與先前發送至用戶端相同的或可經修改。在任一情形中，在1159處，將新隨機詢問及逾期指示發送至安全事務服務101。

圖11B中所展示之事務圖之其餘部分以實質上如上文所闡述(參見例如**圖5**)之相同方式操作。舉例而言，在1160處，顯示一認證使用者介面(例如，引導使用者來在一指紋感測器上撥動一手指)且在1161處，使用者提供認證(例如，在指紋掃描器上撥動一手指)。在1162處，安全事務服務驗證使用者之身分識別(例如，比較自使用者收集之認證資料與儲存於安全儲存裝置720中之彼認證資料)且使用與認證裝置相關聯之密鑰來加密隨機詢問。在1163處，將使用者名稱(或其他ID碼)及經加密隨機詢問發送至伺服器130。最後，在1164處，伺服器130使用使用者名稱(或其他ID碼)識別安全事務資料庫120內之使用者，且使用儲存於安全事務資料庫120中之密鑰解密/驗證隨機詢問來完成認證程序。

用於實施之系統及方法

一認證框架內之隱私類別

在一項實施例中，隱私保護之多個類別可由終端使用者預定義、選擇及/或修改。可基於可使用洩漏資訊識別一用戶端之概率定義隱私類別。在具有相對較高隱私等級之隱私類別下，關於用戶端裝

置之相對較少資訊經洩漏以執行本文中所闡述之認證技術。在一項實施例中，使用者可在與不同伺服器通信時選擇揭示儘可能最小量之資訊(亦即，可選擇具有對每一網站或網路服務最低可允許隱私影響之事務)。

圖12圖解說明用於實施隱私類別之一高等級架構。如所圖解說明，此實施例之安全事務服務101包含隱私管理邏輯1201，該隱私管理邏輯用於分析自伺服器130接收之對用戶端資訊(諸如與認證裝置相關之資訊)之查詢、回應於此等查詢實施一隱私原則及產生含有基於使用中之特定隱私類別收集之用戶端資訊之一回應。在一項實施例中，隱私管理模組1201實施為執行於安全事務服務101之內容脈絡內之一軟體模組。然而，應注意，隱私管理模組1201可以任何方式實施而仍遵守本發明之基本原理且可包含軟體、硬體、韌體或其任何組合。

由隱私管理邏輯1201利用之隱私類別可經預先規定且儲存於用戶端100上(例如，儲存於安全儲存裝置720內)。在一項實施例中，三個隱私類別經定義：高隱私影響、中隱私影響及低隱私影響。可基於可使用洩漏資訊來唯一地識別一使用者/用戶端之一概率定義每一隱私類別。舉例而言，針對一低隱私影響事務洩漏之資訊可產生使用者或機器經由網際網路唯一地經識別之一10%概率；一中隱私影響事務可產生使用者或機器唯一地經識別之一50%概率；且一高隱私影響事務可產生使用者或機器唯一地經識別之一100%概率。可定義各種其他隱私類級而仍遵守本發明之基本原理。

在一項實施例中，每一依賴方(例如，每一網站131或服務151)可

規定一所需要隱私類別或其他隱私臨限值。舉例而言，需要一提高之安全性等級之網站及服務可僅允許根據高隱私影響類別之通信而其他網站/服務可准許使用中隱私影響或低隱私影響類別之互動。在一項實施例中，對自伺服器130發送之用戶端資訊之查詢包含規定應擷取資訊之哪些隱私類別(亦即低、中、高)之一屬性。因此，隱私管理邏輯1201將儲存每一依賴方之最高經核准之隱私類別之資訊。在一項實施例中，每當依賴方請求屬於比已經核准之類別高之一隱私類別之資訊時，使用者將經提示以永久地核准(或拒絕)此依賴方之此新隱私類別。回應於使用者之核准，隱私管理邏輯可儲存依賴方(例如，經由一URL識別)與新隱私類別之間的新關聯。

儘管為簡明起見將使用者偏好1230直接施加至**圖12**中之隱私管理邏輯，但應注意，使用者可經由一基於瀏覽器圖形使用者介面(未展示)規定偏好。在此一情形中，使用者將經由一瀏覽器窗鍵入隱私設定。安全事務外掛程式105將接著將新設定儲存至隱私管理邏輯1201或至可由隱私管理邏輯1201存取之一組態資料文件。簡而言之，本發明之基本原理不限於用於組態隱私管理邏輯之任何特定機制。

可在各種隱私類級下規定各種類型之用戶端資料，包含(舉例而言)一機器型號識別符、用戶端軟體資訊、用戶端能力及與組態於用戶端裝置上之每一認證裝置相關之各種等級之資訊(例如，裝置ID碼、供應商ID碼、裝置類別ID等)。此資訊之不同組合可經聚集以判定上文所規定之定義不同隱私類別之百分比。

圖13圖解說明用於使用經定義隱私類別將資訊提供至一請求方之一系列事務。在1301處，伺服器130產生含有對用戶端裝置資訊之

一查詢之一通知。在1302處，查詢發送至用戶端且最終由安全事務服務101接收。在1303處，安全事務服務之隱私管理邏輯判定回應之一隱私類別且收集必要資訊。如上文所提及，N個不同隱私類級可經定義且安全事務服務101可選擇遵守請求方之要求同時洩漏儘可能少之關於用戶端資訊之一者。在1304處，所收集資訊發送至伺服器130且在1305處，伺服器使用資訊以用於與用戶端之一或多個後續事務。

用於使用事務簽章實施一認證框架之系統及方法

本發明之一項實施例採用在安全事務伺服器上簽章之事務以使得不需要事務狀態維持於伺服器上以維持與用戶端之工作階段。特定而言，經簽章之諸如事務文字之事務細節可藉由伺服器發送至用戶端。伺服器可接著驗證由用戶端接收之經簽章事務回應係藉由驗證簽章有效的。伺服器不需要持續儲存事務內容，持續儲存事務內容將為大量用戶端耗用一顯著量之儲存空間且將創造伺服器上之服務拒絕類型攻擊之可能性。

本發明之一項實施例圖解說明於**圖14**中，其展示起始與一用戶端100之一事務之一網站或其他網路服務(1401)。舉例而言，使用者可已選擇在網站上購買之物項且可準備結帳及支付。在所圖解說明之實例中，網站或服務1401將事務遞交給一安全事務伺服器1402，該安全事務伺服器包含用於產生及驗證簽章(如本文中所闡述)之簽章處理邏輯1403及用於執行用戶端認證1404 (例如，使用先前所闡述之認證技術)之認證邏輯。

在一項實施例中，自安全事務伺服器1402發送至用戶端100之認證請求包含諸如一密碼編譯臨時用法(如上文所闡述)之隨機詢問、事

務細節(例如，用以完成事務所呈現之特定文字)及由簽章處理邏輯1403經由隨機詢問及事務細節使用一私密密鑰(僅由安全事務伺服器已知)產生之一簽章。

一旦上文資訊由用戶端接收，使用者便可接收需要認證來完成事務之一指示。作為回應，使用者可(舉例而言)跨越一指紋掃描器撥動一手指、抓拍一圖片、對一麥克風講話或執行既定事務准許之任何其他類型之認證。在一項實施例中，一旦使用者已在用戶端100上成功地認證，用戶端便將以下內容傳輸回至伺服器：(1)隨機詢問及事務文字(皆由伺服器先前提供至用戶端)、(2)證明使用者成功地完成認證之認證資料及(3)簽章。

安全事務伺服器1402上之認證模組1404可接著確認使用者已正確地經認證且簽章處理邏輯1403經由隨機詢問及事務文字使用私密密鑰重新產生簽章。若簽章匹配由用戶端發送之一者，則伺服器可驗證事務文字與其自網站或服務1401最初經接收時係相同的。保留儲存及處理資源，此乃因不需要安全事務伺服器1402將事務文字(或其他事務資料)持續儲存於安全事務資料庫120內。

例示性資料處理裝置

圖15係圖解說明可用於本發明之某些實施例中之一例示性用戶端及伺服器之一方塊圖。應理解，儘管**圖15**圖解說明一電腦系統之各種組件，但其不意欲表示互連組件之任何特定架構或方式，此乃因此等細節係對本發明不恰當的。將瞭解，具有較少組件或較多組件之其他電腦系統亦可與本發明一起使用。

如**圖15**中所圖解說明，電腦系統1500 (其係一資料處理系統之一

形式)包含與處理系統1520、電源供應器1525、記憶體1530及非揮發性記憶體1540 (例如，一硬碟機、快閃記憶體、相變記憶體(PCM)等)耦合在一起之匯流排1550。匯流排1550可透過各種橋、控制器及/或配接器彼此連接，如此項技術中眾所周知。處理系統1520可自記憶體1530及/或非揮發性記憶體1540擷取指令且執行指令以執行如上文所闡述之操作。匯流排1550將上文組件互連在一起且亦將彼等組件互連至選用銜接塢1560、顯示控制器及顯示裝置1570、輸入/輸出裝置1580 (例如，NIC (網路介面卡)、一游標控制裝置(例如，滑鼠、觸控螢幕、觸控板等)、一鍵盤等)及選用無線收發器1590 (例如，藍芽、WiFi、紅外線等)。

圖16係圖解說明可用於本發明之某些實施例中之一例示性資料處理系統之一方塊圖。舉例而言，資料處理系統1600可係一手持電腦、一個人數位助理(PDA)、一行動電話、一可攜式遊戲系統、一可攜式媒體播放器、一平板或可包含一行動電話之一手持計算裝置、一媒體播放器及/或一遊戲系統。作為另一實例，資料處理系統1600可係另一裝置內之一網路電腦或一嵌入式處理裝置。

根據本發明之一項實施例，資料處理系統1600之例示性架構可用於上文所闡述之行動裝置。資料處理系統1600包含處理系統1620，該處理系統可包含一或多個微處理器及/或一積體電路上之一系統。處理系統1620與一記憶體1610、一電源供應器1625 (其包含一或多個電池)、一音訊輸入/輸出1640、一顯示控制器及顯示裝置1660、選用輸入/輸出1650、輸入裝置1670及無線收發器1630耦合在一起。將瞭解，在本發明之特定實施例中，額外組件(**圖16**中未展示)亦可係資料

處理系統1600之一部分，且在本發明之特定實施例中，可使用比**圖16**中所展示之組件少之組件。另外，將瞭解，一或多個匯流排(**圖16**中未展示)可用以互連如在此項技術中眾所周知之各種組件。

記憶體1610可儲存供由資料處理系統1600執行之資料及/或程式。音訊輸入/輸出1640可包含一麥克風及/或一揚聲器以透過揚聲器及麥克風(舉例而言)播放音樂及/或提供電話功能性。顯示控制器及顯示裝置1660可包含一圖形使用者介面(GUI)。無線(例如，RF)收發器1630 (例如，一WiFi收發器、一紅外線收發器、一藍芽收發器、一無線蜂巢式電話收發器等)可用以與其他資料處理系統通信。一或多個輸入裝置1670允許一使用者將輸入提供至系統。此等輸入裝置可係一小鍵盤、鍵盤、觸控面板、多觸控面板等。選用其他輸入/輸出1650可係用於一銜接塢之一連接器。

本發明之實施例可包含如上文陳述之各種步驟。步驟可體現於機器可執行指令中，該等指令致使一一般用途或特殊用途處理器執行特定步驟。另一選擇係，此等步驟可由含有用於執行步驟之硬佈線邏輯之特定硬體組件或由經程式化電腦組件及定製硬體組件之任何組合執行。

本發明之元件亦可提供為用於儲存機器可執行程式碼之一機器可讀媒體。機器可讀媒體可包含(但不限於)軟式磁片、光碟、CD-ROM及磁光碟、ROM、RAM、EPROM、EEPROM、磁性或光學卡或適合於儲存電子程式碼之其他類型之媒體/機器可讀媒體。

貫穿前述說明，出於闡釋之目的，陳述眾多特定細節以便提供對本發明之一透徹理解。然而，熟習此項技術者將明瞭，可在無此等

特定細節中之某些細節之情況下實踐本發明。舉例而言，熟習此項技術者將易於明瞭，本文中所闡述之功能模組及方法可實施為軟體、硬體或其任何組合。此外，儘管本發明之某些實施例在本文中闡述為在一行動計算環境之內容脈絡內，但本發明之基本原理不限於一行動計算實施方案。可在某些實施例中使用幾乎任何類型之用戶端或同級資料處理裝置，包含(舉例而言)桌上型或工作站電腦。因此，應就以下申請專利範圍判斷本發明之範疇及精神。

【符號說明】

100	用戶端
101	安全事務服務
102	介面/裝置介面/裝置
104	網頁瀏覽器/瀏覽器/用戶端瀏覽器
105	瀏覽器外掛程式/安全事務外掛程式/外掛程式
110	認證裝置
111	認證裝置
112	認證裝置
120	安全儲存裝置/安全事務資料庫/資料庫
130	伺服器/安全企業或網頁目的地/認證裝置/安全事務服務
131	網站/網頁伺服器/網站伺服器
132	安全事務伺服器/內部部署事務伺服器/事務伺服器
133	安全事務伺服器/外部部署事務伺服器
151	網路服務/服務

154	獨立應用程式/應用程式
601	窗
701	原則過濾器
720	安全儲存區域/安全儲存裝置
730	使用者偏好
901	多裝置處理邏輯
902	多裝置處理邏輯
1201	隱私管理邏輯/隱私管理模組
1230	使用者偏好
1401	網站或服務
1402	安全事務伺服器
1403	簽章處理邏輯
1404	用戶端認證/認證模組
1520	處理系統
1525	電源供應器
1530	記憶體
1540	非揮發性記憶體
1550	匯流排
1560	選用銜接塢
1570	顯示控制器及顯示裝置
1580	輸入/輸出裝置
1590	選用無線收發器
1610	記憶體

1620	處理系統
1625	電源供應器
1630	無線收發器
1640	音訊輸入/輸出
1650	選用輸入輸出/選用其他輸入輸出
1660	顯示控制器及顯示裝置
1670	輸入裝置

I635409

【發明摘要】

【中文發明名稱】

判定認證能力之查詢系統、方法及非暫態機器可讀媒體

【英文發明名稱】

QUERY SYSTEM, METHOD AND NON-TRANSITORY MACHINE-READABLE MEDIUM TO DETERMINE AUTHENTICATION CAPABILITIES

【中文】

本發明闡述一種用於判定認證能力之系統、設備、方法及機器可讀媒體。舉例而言，一種方法之一項實施例包括：接收識別一組可接受認證能力之一原則；判定一組用戶端認證能力；且基於該組所判定用戶端認證能力過濾該組可接受認證能力以得出一組經過濾之一或多個認證能力用於認證該用戶端之一使用者。

【英文】

A system, apparatus, method, and machine readable medium are described for determining the authentication capabilities. For example, one embodiment of a method comprises: receiving a policy identifying a set of acceptable authentication capabilities; determining a set of client authentication capabilities; and filtering the set of acceptable authentication capabilities based on the determined set of client authentication capabilities to arrive at a filtered set of one or more authentication capabilities for authenticating a user of the client.

【指定代表圖】

圖7

【發明申請專利範圍】

【第1項】

一種用於判定認證能力之方法，其包括：

偵測一用戶端上之N個認證裝置，其中N>1；

產生N個密碼編譯實體(cryptographic entities)，而該N個認證裝置中之每一者一個密碼編譯實體；

將一單一命令自一伺服器傳輸至該用戶端以將該N個密碼編譯實體中之每一者註冊至該N個認證裝置中之每一者中且將一第一隨機詢問(random challenge)自該伺服器傳輸至該用戶端；

判定N個隱私類別，而該N個認證裝置中之每一者一個隱私類別，其中該隱私類別係基於與該對應認證裝置相關聯之一用戶端資訊唯一地識別一使用者或用戶端裝置之一風險而界定；

在該用戶端上執行該命令且作為回應將該N個密碼編譯實體中之每一者註冊至該用戶端上之該各別N個認證裝置中之每一者中；

在該用戶端處基於與該第一隨機詢問相關聯之一逾期時間(timeout period)而自動偵測該第一隨機詢問不再有效；

作為回應將對一新隨機詢問之一請求自該用戶端傳輸至該伺服器，其中傳輸係在無使用者干預之情況下執行；

在該伺服器處產生一新隨機詢問且將該新隨機詢問傳輸至該用戶端；

以所有該N個認證裝置已註冊之一單一通知將該新隨機詢問傳回至該伺服器，其中該伺服器驗證所接收之該新隨機詢問與所

傳輸之該新隨機詢問相同；及

隨後使用該等認證裝置中之至少一者及其相關聯之密碼編譯實體以用於經由一網路以該伺服器或一不同伺服器認證該用戶端之一使用者，其中用以認證該用戶端之一使用者之該至少一個認證裝置係基於其之對應隱私類別。

【第2項】

如請求項1之方法，其中該密碼編譯實體包括多個密鑰。

【第3項】

如請求項2之方法，其中該等密鑰包括多個對稱密鑰，其中一既定密鑰之一相同複本係儲存於該用戶端上之一安全儲存裝置及與一伺服器相關聯之一安全事務資料庫中。

【第4項】

如請求項2之方法，其中該等密鑰包括多個不對稱密鑰對，其中該密鑰對之一第一密鑰係儲存於該用戶端上之一安全儲存裝置中，且該密鑰對之一第二密鑰係儲存於與一伺服器相關聯之一安全事務資料庫中。

【第5項】

如請求項1之方法，其中使用該等認證裝置中之一者及其相關聯之密碼編譯實體以用於認證一使用者包括：

自該認證裝置接收生物識別使用者輸入；

判定該生物識別使用者輸入成功地認證該使用者；及

使用與該認證裝置相關聯之該密碼編譯實體來加密將發送至一伺服器之資訊。

【第6項】

如請求項1之方法，其中該N個認證裝置中包括多個生物認證裝置，該方法進一步包括：

在產生該N個密碼編譯實體之前，以該用戶端上之該N個認證裝置登記該使用者，而該N個認證裝置中之每一者一個密碼編譯實體。

【第7項】

如請求項1之方法，其中該伺服器使用與一特定認證裝置相關聯之一密碼編譯實體來驗證該用戶端及/或該認證裝置之身分識別。

【第8項】

如請求項2之方法，其中使用一密鑰佈建協定傳輸該等密鑰。

【第9項】

如請求項8之方法，其中該佈建協定包括動態對稱密鑰佈建協定(SDKPP)。

【第10項】

一種用於判定認證能力之系統，其包括用於儲存程式碼之至少一記憶體及用於處理程式碼之至少一處理器以執行以下操作：

偵測一用戶端上之N個認證裝置，其中N>1；

產生N個密碼編譯實體，而該N個認證裝置中之每一者一個密碼編譯實體；

將一單一命令自一伺服器傳輸至該用戶端以將該N個密碼編譯實體中之每一者註冊至該N個認證裝置中之每一者中且將一第一隨機詢問自該伺服器傳輸至該用戶端；

判定N個隱私類別，而該N個認證裝置中之每一者一個隱私類別，其中該隱私類別係基於與該對應認證裝置相關聯之一用戶端資訊唯一地識別一使用者或用戶端裝置之一風險而界定；

在該用戶端上執行該命令且作為回應將該N個密碼編譯實體中之每一者註冊至該用戶端上之該各別N個認證裝置中之每一者中；

在該用戶端處基於與該第一隨機詢問相關聯之一逾期時間而自動偵測該第一隨機詢問不再有效；

作為回應將對一新隨機詢問之一請求自該用戶端傳輸至該伺服器，其中傳輸係在無使用者干預之情況下執行；

在該伺服器處產生一新隨機詢問且將該新隨機詢問傳輸至該用戶端；

以所有該N個認證裝置已註冊之一單一通知將該新隨機詢問傳回至該伺服器，其中該伺服器驗證所接收之該新隨機詢問與所傳輸之該新隨機詢問相同；及

隨後使用該等認證裝置中之至少一者及其相關聯之密碼編譯實體以用於經由一網路以該伺服器或一不同伺服器認證該用戶端之一使用者，其中用以認證該用戶端之一使用者之該至少一個認證裝置係基於其之對應隱私類別。

【第11項】

如請求項10之系統，其中該密碼編譯實體包括多個密鑰。

【第12項】

如請求項11之系統，其中該等密鑰包括多個對稱密鑰，其中一既

定密鑰之一相同複本係儲存於該用戶端上之一安全儲存裝置及與一伺服器相關聯之一安全事務資料庫中。

【第13項】

如請求項11之系統，其中該等密鑰包括多個不對稱密鑰對，其中該密鑰對之一第一密鑰係儲存於該用戶端上之一安全儲存裝置中，且該密鑰對之一第二密鑰係儲存於與一伺服器相關聯之一安全事務資料庫中。

【第14項】

如請求項10之系統，其中使用該等認證裝置中之一者及其相關聯之密碼編譯實體以用於認證一使用者包括：

自該認證裝置接收生物識別使用者輸入；

判定該生物識別使用者輸入成功地認證該使用者；及

使用與該認證裝置相關聯之該密碼編譯實體來加密將發送至一伺服器之資訊。

【第15項】

如請求項10之系統，其中該N個認證裝置中包括多個生物認證裝置，該系統進一步包括：

在產生該N個密碼編譯實體之前，以該用戶端上之該N個認證裝置登記該使用者，而該N個認證裝置中之每一者一個密碼編譯實體。

【第16項】

如請求項10之系統，其中該伺服器使用與一特定認證裝置相關聯之一密碼編譯實體來驗證該用戶端及/或該認證裝置之身分識別。

【第17項】

如請求項11之系統，其中使用一密鑰佈建協定傳輸該等密鑰。

【第18項】

如請求項17之系統，其中該佈建協定包括動態對稱密鑰佈建協定(SDKPP)。

【第19項】

一種具有程式碼儲存於其上之非暫態機器可讀媒體，當由一或多個機器執行時，使該一或多個機器執行以下操作：

偵測一用戶端上之N個認證裝置，其中N>1；

產生N個密碼編譯實體，而該N個認證裝置中之每一者一個密碼編譯實體；

將一單一命令自一伺服器傳輸至該用戶端以將該N個密碼編譯實體中之每一者註冊至該N個認證裝置中之每一者中且將一第一隨機詢問自該伺服器傳輸至該用戶端；

判定N個隱私類別，而該N個認證裝置中之每一者一個隱私類別，其中該隱私類別係基於與該對應認證裝置相關聯之一用戶端資訊唯一地識別一使用者或用戶端裝置之一風險而界定；

在該用戶端上執行該命令且將該N個密碼編譯實體中之每一者分別註冊至該用戶端上之該各別N個認證裝置中之每一者中；

在該用戶端處基於與該第一隨機詢問相關聯之一逾期時間而自動偵測該第一隨機詢問不再有效；

作為回應將對一新隨機詢問之一請求自該用戶端傳輸至該伺服器，其中傳輸係在無使用者干預之情況下執行；

在該伺服器處產生一新隨機詢問且將該新隨機詢問傳輸至該用戶端；

以該N個認證裝置之所有者已註冊之一單一通知將該新隨機詢問傳回至該伺服器，其中該伺服器驗證所接收之該新隨機詢問與所傳輸之該新隨機詢問相同；及

隨後使用該等認證裝置中之至少一者及其相關聯之密碼編譯實體以用於經由一網路以該伺服器或一不同伺服器認證該用戶端之一使用者，其中用以認證該用戶端之一使用者之該至少一個認證裝置係基於其之對應隱私類別。

【第20項】

如請求項19之非暫態機器可讀媒體，其中該密碼編譯實體包括多個密鑰。

【第21項】

如請求項20之非暫態機器可讀媒體，其中該等密鑰包括多個對稱密鑰，其中一既定密鑰之一相同複本係儲存於該用戶端上之一安全儲存裝置及與一伺服器相關聯之一安全事務資料庫中。

【第22項】

如請求項20之非暫態機器可讀媒體，其中該等密鑰包括多個不對稱密鑰對，其中該密鑰對之一第一密鑰係儲存於該用戶端上之一安全儲存裝置中，且該密鑰對之一第二密鑰係儲存於與一伺服器相關聯之一安全事務資料庫中。

【第23項】

如請求項19之非暫態機器可讀媒體，其中使用該等認證裝置中

之一者及其相關聯之密碼編譯實體以用於認證一使用者包括：

自該認證裝置接收生物識別使用者輸入；

判定該生物識別使用者輸入成功地認證該使用者；及

使用與該認證裝置相關聯之該密碼編譯實體來加密將發送至一伺服器之資訊。

【第24項】

如請求項19之非暫態機器可讀媒體，其中該N個認證裝置中包括多個生物認證裝置，該非暫態機器可讀媒體進一步包括：

在產生該N個密碼編譯實體之前，以該用戶端上之該N個認證裝置登記該使用者，而該N個認證裝置中之每一者一個密碼編譯實體。

【第25項】

如請求項19之非暫態機器可讀媒體，其中該伺服器使用與一特定認證裝置相關聯之一密碼編譯實體來驗證該用戶端及/或該認證裝置之身分識別。

【第26項】

如請求項19之非暫態機器可讀媒體，其中使用一密鑰佈建協定傳輸該等密鑰。

【第27項】

如請求項26之非暫態機器可讀媒體，其中該佈建協定包括動態對稱密鑰佈建協定(SDKPP)。

【發明摘要】

【中文發明名稱】

判定認證能力之查詢系統、方法及非暫態機器可讀媒體

【英文發明名稱】

QUERY SYSTEM, METHOD AND NON-TRANSITORY MACHINE-READABLE MEDIUM TO DETERMINE AUTHENTICATION CAPABILITIES

【中文】

本發明闡述一種用於判定認證能力之系統、設備、方法及機器可讀媒體。舉例而言，一種方法之一項實施例包括：接收識別一組可接受認證能力之一原則；判定一組用戶端認證能力；且基於該組所判定用戶端認證能力過濾該組可接受認證能力以得出一組經過濾之一或多個認證能力用於認證該用戶端之一使用者。

【英文】

A system, apparatus, method, and machine readable medium are described for determining the authentication capabilities. For example, one embodiment of a method comprises: receiving a policy identifying a set of acceptable authentication capabilities; determining a set of client authentication capabilities; and filtering the set of acceptable authentication capabilities based on the determined set of client authentication capabilities to arrive at a filtered set of one or more authentication capabilities for authenticating a user of the client.

【指定代表圖】

圖7

【代表圖之符號簡單說明】

100 用戶端

101 安全事務服務

105 瀏覽器外掛程式/安全事務外掛程式/外掛程式

110 認證裝置

111 認證裝置

112 認證裝置

130 伺服器/安全企業或網頁目的地/認證裝置/安全事務服務

701 原則過濾器

720 安全儲存區域/安全儲存裝置

730 使用者偏好