



(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 201828131 A

(43)公開日：中華民國 107 (2018) 年 08 月 01 日

(21)申請案號：106101953

(22)申請日：中華民國 106 (2017) 年 01 月 19 日

(51)Int. Cl. : **G06F21/30 (2013.01)**

(71)申請人：阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES LIMITED
(HK)

香港

(72)發明人：孫元博 (CN)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：34 項 圖式數：14 共 62 頁

(54)名稱

資訊註冊、認證方法及裝置

(57)摘要

本申請公開了一種資訊註冊、認證方法及裝置，所述註冊方法包括：向認證伺服器發送標準資訊註冊請求，接收認證伺服器回饋的第一認證資訊，生成標準資訊獲取請求，將標準資訊獲取請求和第一認證資訊發送至安全資訊應用，獲取安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及標準資訊的身份標識，其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的，將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

指定代表圖：

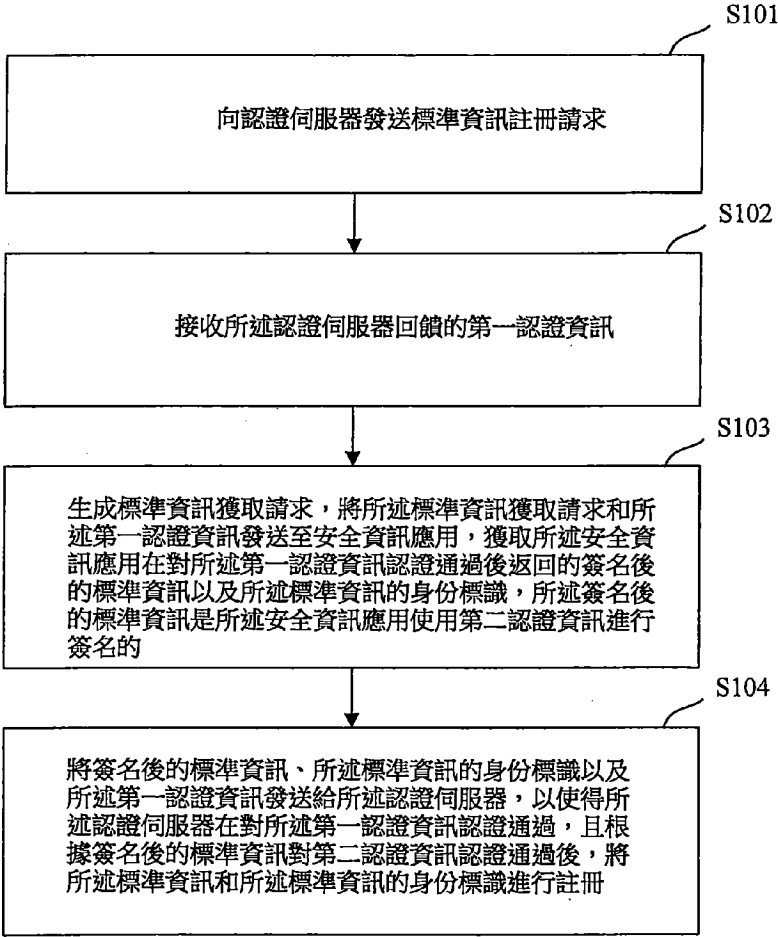


圖 1

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】(中文/英文)

資訊註冊、認證方法及裝置

【技術領域】

本申請係關於電腦技術領域，尤其關於一種資訊註冊、認證方法及裝置。

【先前技術】

隨著資訊技術的發展，用戶可透過終端（如手機、平板電腦等）中安裝的服務提供者（如：軟體發展商、網站等）的應用程式（以下簡稱業務應用），便捷地獲取各類業務服務。對於業務應用中所提供的業務服務而言，某些類別的業務服務具有較高的安全級別，比如：支付業務、轉帳業務等等。安全級別較高的業務服務往往需要用戶提供相應的安全資訊（如：密碼、生物特徵資訊等），並針對用戶提供的安全資訊進行認證後，方可完成業務服務。

對於上述需要用戶提供安全資訊的業務服務而言，通常會在用戶第一次使用該業務服務前，獲取用戶的安全資訊作為標準資訊（標準資訊將作為後續認證過程的認證標準），以便與後續用戶輸入的安全資訊進行比對。在獲取用戶的安全資訊的過程中，業務應用需要透過終端內的安全資訊應用（如：生物資訊管理應用，負責採集、儲存用

戶輸入的生物特徵資訊，該生物資訊管理應用由終端製造商安裝於該終端中）獲取用戶的安全資訊。

為了使得業務應用和安全資訊應用之間進行調用、資訊傳輸時更加便捷，現有技術中，終端系統（如：Android M 系統）將安全資訊應用運行在一種稱為富可執行環境（Rich Execution Environment，REE）的架構中。REE 具備了豐富的調用支援，使得運行在 REE 中的安全資訊應用可更加便捷地被不同的業務應用調用，也可以更加便捷的傳輸各業務應用所需的資訊。

但是，REE 並不屬於安全環境，在安全資訊應用與業務應用進行資訊傳輸的過程中，安全資訊容易被非法操作者在傳輸途中截取並進行篡改。尤其對於標準資訊而言，由於服務提供者在此之前並未保存過用戶提供的標準資訊，也就無法識別標準資訊的真偽，一旦標準資訊在傳輸過程中被篡改，那麼，服務提供者仍會接收被篡改後的標準資訊，並作為後續認證過程中的認證標準，顯然，這將導致非法操作者以用戶的名義獲得各類業務服務。

【發明內容】

本申請實施例提供一種資訊註冊、認證方法及裝置，用以解決現有技術中使用安全資訊進行註冊時安全性較低的問題。

本申請實施例提供的一種資訊註冊方法，包括：

向認證伺服器發送標準資訊註冊請求；

接收所述認證伺服器回饋的第一認證資訊；

生成標準資訊獲取請求，將所述標準資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及所述標準資訊的身份標識，其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的；

將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊註冊方法，包括：

接收業務應用發送的第一認證資訊和標準資訊獲取請求；

對所述第一認證資訊進行認證，並在認證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及所述標準資訊的身份標識返回給所述業務應用，使所述業務應用將簽名後的標準資訊以及所述標準資訊的身份標識發送給認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊註冊方法，包括：

認證伺服器接收業務應用發送的標準資訊註冊請求；

根據所述標準資訊註冊請求，生成第一認證資訊並回饋給所述業務應用；

接收所述業務應用發送的簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊；其中，所述簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給所述業務應用的；

對所述第一認證資訊進行認證，並根據簽名後的標準資訊對所述第二認證資訊進行認證；

在對所述第一認證資訊和所述第二認證資訊認證均通過後，將所述標準資訊以及所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊認證方法，包括：

向認證伺服器發送針對待認證資訊的校驗請求；

接收所述認證伺服器回饋的第一認證資訊；

生成待認證資訊獲取請求，將所述待認證資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的待認證資訊以及所述待認證資訊的待認證身份標識；

將所述待認證資訊、所述待認證身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例還提供的一種資訊認證方法，包括：

接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求；

對所述第一認證資訊進行認證，並在認證通過後，將待認證資訊以及所述待認證資訊的身份標識透過所述業務應用發送至認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例還提供的一種資訊認證方法，包括：

認證伺服器接收業務應用發送的針對待認證資訊的校驗請求；

根據所述校驗請求，生成第一認證資訊並回饋給所述業務應用；

接收所述業務應用發送的待認證資訊、所述待認證資訊的待認證身份標識以及所述第一認證資訊；

分別對所述第一認證資訊、所述待認證身份標識以及所述待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例還提供的一種資訊註冊裝置，包括：

註冊請求模組，用於向認證伺服器發送標準資訊註冊請求；

接收模組，用於接收所述認證伺服器回饋的第一認證資訊；

獲取模組，用於生成標準資訊獲取請求，將所述標準資訊獲取請求和所述第一認證資訊發送至安全資訊應用，

獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及所述標準資訊的身份標識，其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的；

發送模組，用於將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊註冊裝置，包括：

接收模組，用於接收業務應用發送的第一認證資訊和標準資訊獲取請求；

簽名模組，用於對所述第一認證資訊進行認證，並在認證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及所述標準資訊的身份標識返回給所述業務應用，使所述業務應用將簽名後的標準資訊以及所述標準資訊的身份標識發送給認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊註冊裝置，包括：

註冊請求接收模組，用於接收業務應用發送的標準資訊註冊請求；

回饋模組，用於根據所述標準資訊註冊請求，生成第一認證資訊並回饋給所述業務應用；

註冊資訊接收模組，用於接收所述業務應用發送的簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊；其中，所述簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給所述業務應用的；

認證模組，用於對所述第一認證資訊進行認證，並根據簽名後的標準資訊對所述第二認證資訊進行認證；

註冊模組，用於在對所述第一認證資訊和所述第二認證資訊認證均通過後，將所述標準資訊以及所述標準資訊的身份標識進行註冊。

本申請實施例還提供的一種資訊認證裝置，包括：

註冊請求模組，用於向認證伺服器發送針對待認證資訊的校驗請求；

接收模組，用於接收所述認證伺服器回饋的第一認證資訊；

獲取模組，用於生成待認證資訊獲取請求，將所述待認證資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的待認證資訊以及所述待認證資訊的待認證身份標識；

發送模組，用於將所述待認證資訊、所述待認證身份標識以及所述第一認證資訊發送給所述認證伺服器，使得所述認證伺服器對所述第一認證資訊、所述待認證身份

標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例還提供的一種資訊認證裝置，包括：

接收模組，用於接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求；

簽名模組，用於對所述第一認證資訊進行認證，並在認證通過後，將待認證資訊以及所述待認證資訊的身份標識透過所述業務應用發送至認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例還提供的一種資訊認證裝置，包括：

認證請求接收模組，用於接收業務應用發送的針對待認證資訊的校驗請求；

回饋模組，用於根據所述校驗請求，生成第一認證資訊並回饋給所述業務應用；

認證資訊接收模組，用於接收所述業務應用發送的待認證資訊、所述待認證資訊的待認證身份標識以及所述第一認證資訊；

認證模組，用於分別對所述第一認證資訊、所述待認證身份標識以及所述待認證資訊進行認證，生成認證結果回饋給所述業務應用。

本申請實施例提供一種資訊註冊、認證方法及裝置，當用戶在使用業務服務需要註冊標準資訊時，業務應用會向認證伺服器發起標準資訊註冊請求，並接收認證伺服器

所回饋的第一認證資訊，之後，業務應用會生成標準資訊獲取請求和第一認證資訊一併發送給安全資訊應用，在安全資訊應用針對第一認證資訊進行認證通過後，會使用自身的第二認證資訊對標準資訊進行簽名，並確定出該標準資訊的身份標識，再將簽名後的標準資訊及該標準資訊的身份標識回饋給業務應用，從而，業務應用會將安全資訊應用所回饋的，以及第一認證資訊發送給認證伺服器，以便認證伺服器進行認證後，將標準資訊及其身份標識進行註冊。從上述方式中可見，第一認證資訊作為認證伺服器的一種標識，可以使得安全資訊應用確定出標準資訊註冊者的身份；返回認證伺服器的第一認證資訊，使得認證伺服器可以確定出資訊在傳輸途中是否被篡改，而返回認證伺服器的簽名後的標準資訊，使得認證伺服器可以確定出標準資訊是否由終端內的安全資訊應用所提供，這樣的方式可以有效保障認證伺服器可以準確地識別出在傳輸途中被篡改後的標準資訊，有效提升了在註冊標準資訊時的安全性。

【圖式簡單說明】

此處所說明的附圖用來提供對本申請的進一步理解，構成本申請的一部分，本申請的示意性實施例及其說明用於解釋本申請，並不構成對本申請的不當限定。在附圖中：

圖 1 至圖 3 為本申請實施例提供的資訊註冊過程；

圖 4 為本申請實施例提供的在實際應用場景下的資訊註冊過程；

圖 5 至圖 7 為本申請實施例提供的資訊認證過程；

圖 8 為本申請實施例提供的在實際應用場景下的資訊認證過程；

圖 9 至圖 11 為本申請實施例提供的資訊註冊裝置結構示意圖；

圖 12 至圖 14 為本申請實施例提供的資訊認證裝置結構示意圖。

【實施方式】

為使本申請的目的、技術方案和優點更加清楚，下面將結合本申請具體實施例及相應的附圖對本申請技術方案進行清楚、完整地描述。顯然，所描述的實施例僅是本申請一部分實施例，而不是全部的實施例。基於本申請中的實施例，本領域普通技術人員在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬於本申請保護的範圍。

如前所述，當服務提供者第一次接收到標準資訊時，由於之前並未儲存過與該標準資訊相關的安全資訊，所以，也就無法準確地確定出該標準資訊在傳輸過程中是否被篡改。而如果服務提供者與終端之間事先約定了一系列的認證資訊，並使用這些認證資訊對標準資訊進行認證，也就可以識別出標準資訊是否在傳輸過程中被篡改。正是基於此，本申請中提供了下述的資訊註冊和認證方法。

在本申請實施例中，提供了一種資訊註冊方法，如圖 1 所示，該方法包括如下步驟：

S101：向認證伺服器發送標準資訊註冊請求。

在實際應用場景下，當用戶使用業務應用中提供的安全級別較高的業務服務（如：指紋支付業務）時，通常需要用戶提供相應的安全資訊（如：指紋資訊），尤其對於用戶第一次使用該業務服務的情況下，通常需要用戶輸入安全資訊作為標準資訊，用以對用戶後續使用該業務服務時輸入的安全資訊進行對比較驗。

也就是說，在用戶第一使用該業務服務時，需要透過業務應用向相應的認證服務中註冊用戶提供的標準資訊。故在本申請實施例的上述步驟中，由運行在終端內的業務應用向認證伺服器發出標準資訊註冊請求。

其中，本申請中所述的終端包括但不限於：手機、平板電腦、智慧手錶等移動終端，在一些場景中，也可以是電腦終端。所述的認證伺服器，可以是服務提供者後臺服務系統中用以進行安全認證的伺服器，也可以是專門用於進行安全認證的第三方伺服器。當然，這裡並不構成對本申請的限定。

S102：接收所述認證伺服器回饋的第一認證資訊。

所述的第一認證資訊，是由認證伺服器向發出標準資訊註冊請求的業務應用回饋的標識資訊，用以表明認證伺服器的身份。在本申請實施例的一種場景中，第一認證資訊可包括認證服務自身的證書。

S103：生成標準資訊獲取請求，將所述標準資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及所述標準資訊的身份標識。

其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的。

當業務應用接收到了認證伺服器回饋的第一認證資訊後，就會生成標準資訊獲取請求，以請求終端內的安全資訊應用提供註冊所需的標準資訊。

需要說明的是，本申請中的安全資訊應用是運行在終端內的本地應用，用於向業務應用提供業務服務所需的安全資訊（包括標準資訊）。而安全資訊屬於用戶自身的關鍵資訊，為了防止有非法操作者向該安全資訊應用請求用戶的安全資訊，安全資訊應用將對標準資訊的用戶身份進行認證。基於此，當業務應用將標準資訊獲取請求發送至安全資訊應用時，還會將第一認證資訊也發送給安全資訊，從而，安全資訊應用將對第一認證資訊進行認證，以確定認證伺服器的身份。只有在安全資訊應用對第一認證資訊認證通過後，才會提供標準資訊。

考慮到在實際應用中，由安全資訊應用所提供的標準資訊在傳輸的過程中可能被篡改，所以，在本申請中，安全資訊應用在回饋標準資訊之前，將對標準資訊進行簽名操作，用以表明該標準資訊是由該終端內的安全資訊應用所發送的。同時，也考慮到該標準資訊是用戶提供的，故

可以針對該標準資訊，確定該標準資訊的身份標識，用以表明該標準資訊是由用戶提供的。這樣一來，安全資訊應用向業務應用回饋的標準資訊，也就有了兩種標識：分別用來表明該標準資訊是由終端內的安全資訊應用發送的、且該標準資訊是由用戶提供的。

具體而言，本申請中的安全資訊應用會使用第二認證資訊對該標準資訊進行簽名，用以表明該標準資訊是由該安全資訊應用所發送。當然，在本申請中，第二認證資訊可以是認證伺服器與終端內的安全資訊應用（或終端本身）之間預先約定的第二密鑰資訊，這裡並不做具體限定。標準資訊的身份標識也由該安全資訊應用確定，在本申請中，標準資訊的身份標識包括可以表明該標準資訊的身份密鑰資訊，該身份密鑰資訊通常與用戶的帳戶資訊相關聯。也就是說，一對身份密鑰資訊唯一對應一個帳戶資訊，這樣也就能夠表明該標準資訊屬於該用戶。當然，這裡也不做具體限定。

S104：將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

當業務應用接收到安全資訊應用的回饋後，就會將安全資訊應用所回饋的簽名後的標準資訊、該標準資訊的身份標識以及由認證伺服器發送的第一認證資訊，一併發送

給認證伺服器進行認證並註冊。

認證伺服器接收到了業務應用發送的上述資訊後，就會對所接收到的資訊進行認證。如果認證通過，那麼也就表明由安全資訊應用所發送的標準資訊在傳輸途中並未被篡改，從而，認證伺服器也就可以將標準資訊及其身份標識進行註冊。註冊的標準資訊以及身份標識也就可以用來對後續用戶提供的安全資訊進行認證識別。

透過上述步驟，當用戶在使用業務服務需要註冊標準資訊時，業務應用會向認證伺服器發起標準資訊註冊請求，並接收認證伺服器所回饋的第一認證資訊，之後，業務應用會生成標準資訊獲取請求和第一認證資訊一併發送給安全資訊應用，在安全資訊應用針對第一認證資訊進行認證通過後，會使用自身的第二認證資訊對標準資訊進行簽名，並確定出該標準資訊的身份標識，再將簽名後的標準資訊及該標準資訊的身份標識回饋給業務應用，從而，業務應用會將安全資訊應用所回饋的，以及第一認證資訊發送給認證伺服器，以便認證伺服器進行認證後，將標準資訊及其身份標識進行註冊。從上述方式中可見，第一認證資訊作為認證伺服器的一種標識，可以使得安全資訊應用確定出標準資訊註冊者的身份；返回認證伺服器的第一認證資訊，使得認證伺服器可以確定出資訊在傳輸途中是否被篡改，而返回認證伺服器的簽名後的標準資訊，使得認證伺服器可以確定出標準資訊是否由終端內的安全資訊應用所提供，這樣的方式可以有效保障認證伺服器可以準

確地識別出在傳輸途中被篡改後的標準資訊，有效提升了在註冊標準資訊時的安全性。

對於上述的第一認證資訊而言，第一認證資訊是認證伺服器的一種標識，用來標示認證伺服器的身份，具體可以將認證伺服器自身的證書作為第一認證資訊，當然，考慮到傳輸過程中的安全性，認證伺服器可以使用自身的密鑰資訊對其證書進行簽名操作。那麼，作為本申請實施例中的一種可選方式，上述步驟 S102：接收所述認證伺服器回饋的第一認證資訊，具體為：接收所述認證伺服器發送的、採用該認證伺服器自身的第一加密密鑰進行簽名後的證書，並將簽名後的證書作為所述第一認證資訊。

此外，在實際應用中的某些場景下，認證伺服器向業務應用回饋的第一認證資訊中，還包含有挑戰碼。當業務應用向認證伺服器發送一次請求後，認證伺服器就會生成一個具有唯一性的挑戰碼，攜帶在第一認證資訊中回饋給業務應用。可以認為，一個挑戰碼就對應一次業務請求。採用挑戰碼的方式可以防止重放攻擊。

以上內容是基於終端內的業務應用的角度所進行的描述。而對於提供標準資訊的安全資訊應用而言，本申請實施例中還提供了一種資訊註冊過程，如圖 2 所示，該過程包括如下步驟：

S201：接收業務應用發送的第一認證資訊和標準資訊獲取請求。

本實施例中的第一認證資訊和標準資訊獲取請求如前

所述。在此不再敘述。

S202：對所述第一認證資訊進行認證，並在認證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及所述標準資訊的身份標識返回給所述業務應用，使所述業務應用將簽名後的標準資訊以及所述標準資訊的身份標識發送給認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

當安全資訊應用接收到了業務應用發送的第一認證資訊和標準資訊獲取請求後，首先會對第一認證資訊進行認證，以便確定出標準資訊的註冊者的身份。只有在安全資訊應用確定了認證伺服器的身份後，安全資訊應用才會將用戶提供的標準資訊進行簽名，並確定出該標準資訊的身份標識，再將簽名後的標準資訊和該標準資訊的身份標識回饋給業務應用。從而，業務應用將安全資訊應用回饋的一系列資訊和第一認證資訊一併發送給認證伺服器。後續由認證伺服器進行認證，並在認證通過後對標準資訊和該標準資訊的身份標識進行註冊。這裡的內容與上述方法中的過程相同，故在此不再過多贅述。

透過上述步驟，由認證伺服器提供的第一認證資訊可以標示出認證伺服器的身份，安全資訊應用對第一認證資訊的認證，可以避免非法操作者向該安全資訊應用獲取標準資訊。而安全資訊應用對用戶提供的標準資訊進行簽名

的方式，是用來表明該標準資訊是由安全資訊應用發送的，同時確定出該標準資訊的身份標識，用來表明該標準資訊由該用戶提供，顯然，安全資訊應用回饋給業務應用的標準資訊中包含了兩種標識，而如果標準資訊在傳輸過程中被篡改，那麼，標準資訊的兩種標識都將會發生改變。這樣的方式可以有效地反映出標準資訊在傳輸過程中是否被篡改，也就保證了最終認證伺服器在註冊時的安全性。

將使用第二認證資訊進行簽名後的標準資訊，以及所述標準資訊的身份標識返回給所述業務應用，具體為：接收用戶輸入的標準資訊，使用第二認證資訊對所述標準資訊進行簽名，並針對所述標準資訊，確定所述標準資訊的身份標識，將簽名後的標準資訊以及所述標準資訊的身份標識，返回給所述業務應用。

如前所述，本申請中標準資訊的身份標識，具體可以包括該標準資訊的身份密鑰資訊，該身份密鑰資訊通常與用戶的帳戶資訊相關聯。在傳輸過程中，為了保證該身份密鑰資訊的安全性，在本申請實施例中的一種可選方式下，安全資訊應用也可以使用第二認證資訊對所述身份密鑰資訊（亦即，標準資訊的身份標識）進行簽名。當然，這裡並不構成對本申請的限定。

同樣，正如前述，第一認證資訊可表明認證伺服器的身份，而在本申請中的一種方式下，第一認證資訊包括認證伺服器自身的證書，此時，對所述第一認證資訊進行認

證，具體為：使用與所述認證伺服器的第一加密密鑰相匹配的第一解密密鑰對所述簽名後的證書進行解密認證。

對於第二認證資訊而言，在本申請實施例中的一種方式下，所述第二認證資訊包括預先與認證伺服器約定的第二密鑰資訊，其中，所述第二密鑰資訊中包括第二加密密鑰和第二解密密鑰，在此場景下，使用第二認證資訊對所述標準資訊進行簽名，具體為：針對所述標準資訊，使用預先與認證伺服器約定的第二加密密鑰進行簽名。

當然，在標準資訊的身份標識包括該標準資訊的身份密鑰資訊的情況下，還可以使用上述第二認證資訊對身份密鑰資訊進行簽名。這裡與上述方式中的內容類別似，故在此不再過多贅述。

以上內容是基於運行在終端內的安全資訊應用角度的描述，而對於認證伺服器而言，本申請實施例中還提供一種資訊註冊過程，如圖3所示，具體包括以下步驟：

S301：認證伺服器接收業務應用發送的標準資訊註冊請求。

S302：根據所述標準資訊註冊請求，生成第一認證資訊並回饋給所述業務應用。

S303：接收所述業務應用發送的簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊；其中，所述簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給所述業務應用的。

S304：對所述第一認證資訊進行認證，並根據簽名後

的標準資訊對所述第二認證資訊進行認證。

S305：在對所述第一認證資訊和所述第二認證資訊認證均通過後，將所述標準資訊以及所述標準資訊的身份標識進行註冊。

與上述如圖 1 和圖 2 所示的方法相類似，認證伺服器會在接收到業務應用發送的標準資訊註冊請求後，將向業務應用回饋可表明該認證伺服器自身身份的第一認證資訊，使得業務應用向安全資訊發送標準資訊獲取請求後，安全資訊應用可以根據第一認證資訊，確定出認證伺服器的身份，從而，安全資訊應用才會向業務應用回饋使用第二認證資訊簽名後的標準資訊和該標準資訊的身份標識。當認證伺服器接收到了業務應用返回的簽名後的標準資訊和第一認證資訊後，便會對第一認證資訊進行認證，並根據簽名後的標準資訊對第二認證資訊進行認證，如果認證均通過，那麼，也就表明標準資訊在傳輸過程中並未被篡改，從而，認證伺服器會將標準資訊及其身份標識進行註冊，以便後續過程進行認證識別。

正如前述內容所述，認證伺服器自身的證書可有效證明該認證伺服器的身份，而為了保證安全資訊應用接收到的證書的有效性，認證伺服器通常會對其自身的證書進行簽名，從而，如果該證書在傳輸過程中被篡改，安全資訊應用就可以識別出來，故針對上述步驟 S302 而言，根據所述標準資訊註冊請求，生成第一認證資訊並回饋給所述業務應用，具體為：根據所述標準資訊註冊請求，調取該

認證伺服器自身的證書，使用自身的第一加密密鑰對所述證書進行簽名，作為第一認證資訊，並回饋給所述業務應用。

與前述方法中的內容相類似，在本申請實施例的一種場景下，認證伺服器還可以將挑戰碼也攜帶在第一認證資訊中，並使用自身的第一加密密鑰簽名後發送給業務應用。這裡並不構成對本申請的限定。

當業務應用向認證伺服器返回了簽名後的標準資訊和第一認證資訊後，認證伺服器也就會對第一認證資訊進行認證，並根據簽名後的標準資訊對第二認證資訊進行認證。

具體而言，對第一認證資訊進行認證，具體包括：使用第一解密密鑰對所述第一認證資訊進行解密認證。認證伺服器將使用自身的第一解密密鑰對第一認證資訊進行解密認證，如果解密後的證書（或挑戰碼）發生了變化，那麼，就表明在傳輸的過程中極有可能被篡改，從而，認證伺服器將判定為認證不通過。而如果認證伺服器在解密後，證書（或挑戰碼）未發生變化，那麼就通過認證。

對於第二認證資訊而言，與前述方法中的內容相類似，所述第二認證資訊包括預先由所述認證伺服器與所述安全資訊應用約定的第二密鑰資訊；其中，所述第二密鑰資訊包括：第二加密密鑰和第二解密密鑰。此外，簽名後的標準資訊是由所述安全應用使用第二加密密鑰進行簽名的。在這種場景下，根據簽名後的標準資訊對所述第二認

證資訊進行認證，具體為：根據預先約定的第二密鑰資訊，使用與所述安全資訊應用預先約定的第二解密密鑰，對簽名後的標準資訊進行解密，以便對所述第二認證資訊進行認證。

如果認證伺服器使用約定的第二解密密鑰針對簽名後的標準資訊進行解密，並獲得了標準資訊，那麼，就可以認為標準資訊在傳輸的過程中並未被篡改，從而通過認證。而如果進行解密後，得到的是無法使用的資訊，則表明簽名的資訊並不是採用預先約定的第二加密密鑰進行簽名的，這就極有可能是被篡改後的資訊，從而認證不通過。

只有在認證伺服器進行認證通過之後，認證伺服器才會將標準資訊和該標準資訊的身份標識進行註冊。

透過上述如圖 1 至圖 3 所示的資訊註冊方法，使得認證伺服器可以有效地識別出標準資訊在傳輸過程中是否被篡改，也就保證了用戶能夠在使用業務服務時不被非法操作者所影響。

當然，針對上述資訊註冊方法，可適用於任意終端透過業務應用獲取業務服務的場景中，且上述的認證伺服器可以是服務提供者後臺服務系統內的具有認證功能的伺服器。而考慮到實際應用場景中，對於可提供諸如支付業務、轉帳業務等對安全級別要求較高的業務服務的服務提供者而言，通常使用一種稱為互聯網金融身份認證聯盟（Internet Finance Authentication Alliance，IFAA）的網

路身份認證架構，實現對安全級別要求較高的業務服務所需的身份認證支持。亦即，由 IFAA 提供認證伺服器，實現上述的註冊過程。

在這樣的場景下，不同的設備製造廠商也會採用 IFAA 所提供的身份認證架構，在其生產的終端中提供身份認證必備的介面或服務。

為了清楚的闡述本申請中的上述註冊方法，現以 IFAA 提供的身份認證架構中進行註冊為例，進行詳細說明。

如圖 4 所示，為本示例中終端和 IFAA 認證伺服器之間進行註冊的實際應用過程。其中，終端內運行有業務應用和安全資訊應用，業務應用作為某服務提供者的業務服務接入口，可為使用該終端的用戶提供各類業務服務，而安全資訊應用用於為業務應用提供所需的安全資訊（在本示例中為標準資訊）。圖 4 中所示的過程具體包括如下步驟：

S401：業務應用向 IFAA 認證伺服器發送標準資訊註冊請求。

當用戶在終端中第一次使用該業務應用中的某業務服務時，就需要在 IFAA 認證伺服器中註冊該用戶的生物資訊，作為標準資訊。此時，業務應用就會向 IFAA 認證伺服器發出標準資訊註冊請求。

S402：IFAA 認證伺服器將簽名後的包含挑戰碼和證書的資料包回饋給業務應用。

其中，挑戰碼可以防止重放攻擊，證書用以表明該 IFAA 認證伺服器自身的身份。可以認為，經過簽名後的資料包就是上述註冊方法中所述的第一認證資訊。

另外，需要說明的是，本步驟中，IFAA 認證伺服器使用 IFAAS 密鑰資訊對上述的資料包進行簽名，該 IFAAS 密鑰資訊由 IFAA 認證伺服器自身生成。而 IFAA 認證伺服器自身的證書由 BIOM 密鑰資訊進行簽名，BIOM 密鑰資訊用於表明提供該業務服務的服務提供者的類別。

S403：業務應用生成標準資訊獲取請求，並將該標準資訊獲取請求和簽名後的資料包透過 IFAAService 發送給安全資訊應用。

其中，IFAAService 是設置於終端內的 IFAA 身份認證架構所提供的一種服務。當然，在實際應用場景中的一種方式下，業務應用可透過 IFAASDK（一種基於 IFAA 身份認證架構下的通信工具）調用 IFAAService，這裡並不做具體限定。

S404：安全資訊應用對簽名後的資料包進行認證，在認證通過後，將標準資訊進行簽名。

需要說明的是，安全資訊應用首先要對簽名後的資料包進行解密（具體可以使用 IFAA 密鑰資訊進行解密，這裡不作具體限定），在解密後，將認證資料包中的證書（可使用 BIOM 密鑰資訊對證書進行解密認證），以認證是不是 IFAA 將註冊標準資訊。

在認證通過後，安全資訊應用將獲得用戶輸入的生物資訊，作為標準資訊，並使用 DA 密鑰資訊對標準資訊進行簽名。其中，DA 密鑰資訊用於表明該終端的身份（在一種情況下，DA 密鑰資訊可表明安全資訊應用的身份，而安全應用資訊是設備製造商設置於該終端內的，所以，DA 密鑰資訊也表明終端的身份）。

S405：根據簽名後的標準資訊，確定該標準資訊的身份密鑰資訊。

在本示例中，標準資訊的身份密鑰資訊通常與用戶在業務應用中所使用的帳戶資訊相關聯，用以表明該標準資訊所屬的用戶。實際應用中，標準資訊的身份密鑰資訊的生成，可由 IFAAService 透過 KeyStore（一種 REE 環境下的安全儲存標準調用介面）調用 KeyMaster（一種安全儲存模組），並由 KeyMaster 生成該身份密鑰資訊。

需要說明的是，為了保證身份密鑰資訊在傳輸過程中的安全性，安全資訊應用可以使用 DA 密鑰資訊對身份密鑰資訊進行簽名。

S406：安全資訊應用將終端證書、簽名後的標準資訊、簽名後的身份密鑰資訊返回給業務應用。

S407：透過 IFAAService 將終端證書、簽名後的標準資訊、簽名後的身份密鑰資訊發送給 IFAA 認證伺服器。

需要說明的是，終端證書也稱為 authenticator 證書，是參與 IFAA 身份認證架構的設備製造商為其生產的設備中所設置的，亦即，終端證書可以表明該終端是否使用了

IFAA 的身份認證架構。

當然，在本示例的一種方式下，同時返回 IFAA 認證伺服器的還有前述的挑戰碼和 IFAA 認證伺服器自身的證書，這樣一來，IFAA 認證伺服器還可對挑戰碼和 IFAA 認證伺服器自身的證書進行認證。

S408：IFAA 認證伺服器對接收到的資訊進行認證，在認證通過後，將標準資訊及其身份密鑰資訊進行註冊。

需要說明的是，IFAA 認證伺服器首先將對終端證書進行認證，具體可使用 IFAA 密鑰資訊對接收到的資訊進行解密，並認證終端證書的合法性，通過後，將使用 DA 密鑰資訊對身份密鑰資訊進行解密認證，通過後，再對簽名的標準資訊使用 DA 密鑰資訊進行解密認證，均通過後，那麼，就可以認為標準資訊在傳輸途中未被篡改，則 IFAA 認證伺服器將標準資訊及其身份密鑰資訊進行註冊。

S409：向業務應用回饋註冊結果。

透過上例可見，在實際應用場景下，可以使用多種密鑰資訊來準確確定出標準資訊在傳輸過程中是否被篡改。

以上內容是標準資訊的註冊方法，在註冊了標準資訊後，用戶便可以使用相應的業務服務，當用戶使用業務服務時，就需要提供用戶的安全資訊，相應地，認證伺服器也就可以根據用戶在使用業務服務時所提供的安全資訊進行認證。故在本申請實施例中，還提供了一種資訊認證方法，如圖 5 所示，所述方法包括如下步驟：

S501：向認證伺服器發送針對待認證資訊的校驗請求。

當用戶使用業務應用中的業務服務（如：指紋支付業務）時，往往需要用戶提供自身的安全資訊（如：指紋資訊），與之前註冊的標準資訊進行比對。此時，業務應用將會獲取用戶的安全資訊，作為待認證資訊，後續將發送至認證伺服器中進行認證校驗。

在上述情況下，業務應用就會向認證伺服器發送待認證資訊的校驗請求。

S502：接收所述認證伺服器回饋的第一認證資訊。

與前述註冊方法中類似，第一認證資訊表明了認證伺服器的身份。在此不再過多贅述。

S503：根據所述第一認證資訊，生成待認證資訊獲取請求發送至安全資訊應用，獲取由所述安全資訊應用提供的待認證資訊，以及所述待認證資訊的待認證身份標識。

類似地，安全資訊應用將根據第一認證資訊確定出認證者的身份，在確定了認證者的身份合法後，通過認證，再將用戶提供的待認證資訊及其待認證身份標識一併返回給業務應用。

與前述註冊方法中不同的是，對於待認證資訊而言，無需使用第二認證資訊進行簽名。

S504：將所述待認證資訊、所述待認證身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及

待認證資訊進行認證，生成認證結果回饋給所述業務應用。

從上述內容中可以看出，透過第一認證資訊和待認證身份標識，可以識別出待認證資訊是否在傳輸過程中被篡改，在認證通過後，認證伺服器才會對待認證資訊進行認證。

在本申請實施例中，還提供一種資訊認證方法，如圖6所示，該方法包括如下步驟：

S601：接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求。

S602：根據攜帶有第一認證資訊的標準資訊獲取請求，將待認證資訊以及所述待認證資訊的身份標識透過所述業務應用發送至認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

對於上述步驟 S602，根據攜帶有第一認證資訊的標準資訊獲取請求，將待認證資訊以及所述待認證資訊的身份標識返回給所述業務應用，具體為：對所述標準資訊獲取請求中攜帶的所述第一認證資訊進行認證，在認證通過後，接收用戶輸入的待認證資訊，識別所述待認證資訊所屬的標準資訊，將與所述標準資訊相匹配的身份標準確定為該待認證資訊的待認證身份標識，將所述待認證資訊以及所述待認證資訊的待認證身份標識返回給所述業務應用。

在本申請實施例中，還提供一種資訊認證方法，如圖7所示，該方法包括如下步驟：

S701：認證伺服器接收業務應用發送的針對待認證資訊的校驗請求。

S702：根據所述校驗請求，生成第一認證資訊並回饋給所述業務應用。

S703：接收所述業務應用發送的待認證資訊、所述待認證資訊的身份標識以及所述第一認證資訊。

S704：分別對所述第一認證資訊、所述身份標識以及所述待認證資訊進行認證，生成認證結果回饋給所述業務應用。

需要說明的是，對於上述步驟 S704 而言，認證伺服器將對業務應用發送的資訊分別進行認證，具體而言，分別對所述第一認證資訊、所述身份標識以及所述待認證資訊進行認證，具體為：針對所述第一認證資訊，使用自身的第一解密密鑰對所述第一認證資訊進行解密，對解密後的所述證書進行認證，對所述身份標識，根據已註冊的標準資訊的身份標識，判斷所述身份標識是否與已註冊的標識資訊的身份標識相匹配，針對所述待認證資訊，與已註冊的標準資訊進行比對認證。

在實際應用場景中，認證伺服器在認證的過程中，如果有任一資訊的認證未通過，那麼，認證伺服器就可以回饋失敗通知，而只有當所有資訊均通過認證後，才會回饋成功通知。那麼，具體而言，生成認證結果回饋給所述業

務應用，具體為：針對所述第一認證資訊，若認證通過，則對所述待認證資訊及待認證身份標識進行認證；否則，返回認證失敗通知；針對所述身份標識，若認證通過，則對所述待認證資訊進行認證；否則，返回認證失敗通知；針對所述待認證資訊，若認證成功，則返回成功通知；否則，則返回認證失敗通知。

與上述註冊過程相對應，為了清楚的闡述本申請中的上述認證方法，現以 IFAA 提供的身份認證架構中進行認證為例，進行詳細說明。

如圖 8 所示，為本示例中終端和 IFAA 認證伺服器之間進行認證的實際應用過程。所示的過程具體包括如下步驟：

S801：業務應用向 IFAA 認證伺服器發送待認證資訊校驗請求。

S802：IFAA 認證伺服器將簽名後的包含挑戰碼和證書的資料包回饋給業務應用。

S803：業務應用生成待認證資訊獲取請求，並將該待認證資訊獲取請求和簽名後的資料包透過 IFaaSService 發送給安全資訊應用。

S804：安全資訊應用對簽名後的資料包進行認證，在認證通過後，將待認證資訊使用註冊過程中的身份密鑰資訊進行簽名。

S805：安全資訊應用將簽名後的待認證資訊返回給業務應用。

S806：透過 IFaaSService 將簽名後的待認證資訊發送給 IFAA 認證伺服器。

S807：IFAA 認證伺服器針對接收到的簽名後的待認證資訊，使用註冊的身份密鑰資訊對簽名後的待認證資訊進行認證，通過後，將待認證資訊與已註冊標準資訊進行比對認證。

S808：向業務應用返回認證結果。

以上為本申請實施例提供的資訊傳輸方法，基於同樣的思路，本申請實施例還提供一種資訊註冊裝置，如圖 9 所示，所述裝置包括：

註冊請求模組 901，用於向認證伺服器發送標準資訊註冊請求。

接收模組 902，用於接收所述認證伺服器回饋的第一認證資訊。

獲取模組 903，用於生成標準資訊獲取請求，將所述標準資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及所述標準資訊的身份標識，其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的。

發送模組 904，用於將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過

後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

所述接收模組 902，具體用於接收所述認證伺服器發送的、採用該認證伺服器自身的第一加密密鑰進行簽名後的證書，並將簽名後的證書作為所述第一認證資訊。

如圖 10 所示，本申請實施例還提供一種資訊註冊裝置，所述裝置包括：

接收模組 1001，用於接收業務應用發送的第一認證資訊和標準資訊獲取請求；

簽名模組 1002，用於對所述第一認證資訊進行認證，並在認證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及所述標準資訊的身份標識返回給所述業務應用，使所述業務應用將簽名後的標準資訊以及所述標準資訊的身份標識發送給認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

所述簽名模組 1002，具體用於接收用戶輸入的標準資訊，使用第二認證資訊對所述標準資訊進行簽名，並針對所述標準資訊，確定所述標準資訊的身份標識，將簽名後的標準資訊以及所述標準資訊的身份標識，返回給所述業務應用。

需要說明的是，所述標準資訊的身份標識，包括所述標準資訊的身份密鑰資訊，該身份密鑰資訊與所述用戶的

帳戶資訊相關聯。

在所述第一認證資訊中包括認證伺服器簽名後的證書的場景下，所述簽名模組 1002，具體用於使用與所述認證伺服器的第一加密密鑰相匹配的第一解密密鑰對所述簽名後的證書進行解密認證。

所述第二認證資訊包括預先與認證伺服器約定的第二密鑰資訊，其中，所述第二密鑰資訊中包括第二加密密鑰和第二解密密鑰，所述簽名模組 1002，具體用於針對所述標準資訊，使用預先與認證伺服器約定的第二加密密鑰進行簽名。

如圖 11 所示，本申請實施例還提供一種資訊註冊裝置，所述裝置包括：

註冊請求接收模組 1101，用於接收業務應用發送的標準資訊註冊請求；

回饋模組 1102，用於根據所述標準資訊註冊請求，生成第一認證資訊並回饋給所述業務應用；

註冊資訊接收模組 1103，用於接收所述業務應用發送的簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊；其中，所述簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給所述業務應用的；

認證模組 1104，用於對所述第一認證資訊進行認證，並根據簽名後的標準資訊對所述第二認證資訊進行認證；

註冊模組 1105，用於在對所述第一認證資訊和所述第二認證資訊認證均通過後，將所述標準資訊以及所述標準資訊的身份標識進行註冊。

具體地，所述回饋模組 1102，具體用於根據所述標準資訊註冊請求，調取該認證伺服器自身的證書，使用自身的第一加密密鑰對所述證書進行簽名，作為第一認證資訊，並回饋給所述業務應用。

所述認證模組 1104，具體用於使用第一解密密鑰對所述第一認證資訊進行解密認證。

所述第二認證資訊包括預先由所述認證伺服器與所述安全資訊應用約定的第二密鑰資訊；其中，所述第二密鑰資訊包括：第二加密密鑰和第二解密密鑰；簽名後的標準資訊是由所述安全應用使用第二加密密鑰進行簽名的。該場景下，所述認證模組 1104，具體用於根據預先約定的第二密鑰資訊，使用與所述安全資訊應用預先約定的第二解密密鑰，對簽名後的標準資訊進行解密，以便對所述第二認證資訊進行認證。

如圖 12 所示，本申請實施例還提供一種資訊認證裝置，所述裝置包括：

認證請求模組 1201，用於向認證伺服器發送針對待認證資訊的校驗請求；

接收模組 1202，用於接收所述認證伺服器回饋的第一認證資訊；

獲取模組 1203，用於生成待認證資訊獲取請求，將

所述待認證資訊獲取請求和所述第一認證資訊發送至安全資訊應用，獲取所述安全資訊應用在對所述第一認證資訊認證通過後返回的待認證資訊以及所述待認證資訊的待認證身份標識；

發送模組 1204，用於將所述待認證資訊、所述待認證身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

如圖 13 所示，本申請實施例還提供一種資訊認證裝置，所述裝置包括：

接收模組 1301，用於接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求；

簽名模組 1302，用於對所述第一認證資訊進行認證，並在認證通過後，將待認證資訊以及所述待認證資訊的身份標識通過所述業務應用發送至認證伺服器，以使得所述認證伺服器對所述第一認證資訊、所述待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給所述業務應用。

具體地，所述簽名模組 1302，具體用於對所述標準資訊獲取請求中攜帶的所述第一認證資訊進行認證，在認證通過後，識別所述待認證資訊所屬的標準資訊，將與所述標準資訊相匹配的身份標準確定為該待認證資訊的待認證身份標識，將所述待認證資訊以及所述待認證資訊的待

認證身份標識返回給所述業務應用。

如圖 14 所示，本申請實施例還提供一種資訊認證裝置，所述裝置包括：

認證請求接收模組 1401，用於接收業務應用發送的針對待認證資訊的校驗請求；

回饋模組 1402，用於根據所述校驗請求，生成第一認證資訊並回饋給所述業務應用；

認證資訊接收模組 1403，用於接收所述業務應用發送的待認證資訊、所述待認證資訊的待認證身份標識以及所述第一認證資訊；

認證模組 1404，用於分別對所述第一認證資訊、所述待認證身份標識以及所述待認證資訊進行認證，生成認證結果回饋給所述業務應用。

所述認證模組 1404，具體用於針對所述第一認證資訊，使用自身的第一解密密鑰對所述第一認證資訊進行解密，對解密後的所述證書進行認證；針對所述待認證身份標識，根據已註冊的標準資訊的身份標識，判斷所述待認證身份標識是否與已註冊的標識資訊的身份標識相匹配；針對所述待認證資訊，與已註冊的標準資訊進行比對認證。

所述認證模組 1404，具體用於針對所述第一認證資訊，若認證通過，則對所述待認證資訊及待認證身份標識進行認證；否則，返回認證失敗通知；針對所述身份標識，若認證通過，則對所述待認證資訊進行認證；否則，

返回認證失敗通知；針對所述待認證資訊，若認證成功，則返回成功通知；否則，則返回認證失敗通知。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入/輸出介面、網路介面和記憶體。

記憶體可能包括電腦可讀媒體中的非永久性記憶體，隨機存取記憶體（RAM）和/或非揮發性記憶體等形式，如唯讀記憶體（ROM）或快閃記憶體（flash RAM）。記憶體是電腦可讀媒體的示例。

電腦可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是電腦可讀指令、資料結構、程式的模組或其他資料。電腦的儲存媒體的例子包括，但不限於相變記憶體（PRAM）、靜態隨機存取記憶體（SRAM）、動態隨機存取記憶體（DRAM）、其他類型的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、電可擦除可程式設計唯讀記憶體（EEPROM）、快閃記憶體或其他記憶體技術、唯讀光碟唯讀記憶體（CD-ROM）、數位多功能光碟（DVD）或其他光學儲存、磁盒式磁帶，磁帶磁片儲存或其他磁性存放裝置或任何其他非傳輸媒體，可用於儲存可以被計算設備訪問的資訊。按照本文中的界定，電腦可讀媒體不包括電腦可讀暫存媒體（transitory media），如調製的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者任何其他變體意在涵蓋非排他性的包含，從而使得包括一系

列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另外的相同要素。

本領域技術人員應明白，本申請的實施例可提供為方法、系統或電腦程式產品。因此，本申請可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本申請可採用在一個或多個其中包含有電腦可用程式碼的電腦可用儲存媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

以上所述僅為本申請的實施例而已，並不用於限制本申請。對於本領域技術人員來說，本申請可以有各種更改和變化。凡在本申請的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本申請的申請專利範圍的範圍之內。

【符號說明】

901：註冊請求模組

902：接收模組

903：獲取模組

904：發送模組

- 1001：接收模組
- 1002：簽名模組
- 1101：註冊請求接收模組
- 1102：回饋模組
- 1103：註冊資訊接收模組
- 1104：認證模組
- 1105：註冊模組
- 1201：認證請求模組
- 1202：接收模組
- 1203：獲取模組
- 1204：發送模組
- 1301：接收模組
- 1302：簽名模組
- 1401：認證請求接收模組
- 1402：回饋模組
- 1403：認證資訊接收模組
- 1404：認證模組

發明摘要

※申請案號：106101953

※申請日：106 年 01 月 19 日

※IPC 分類：G06F 21/30 (2013.01)

【發明名稱】(中文/英文)

資訊註冊、認證方法及裝置

【中文】

本申請公開了一種資訊註冊、認證方法及裝置，所述註冊方法包括：向認證伺服器發送標準資訊註冊請求，接收認證伺服器回饋的第一認證資訊，生成標準資訊獲取請求，將標準資訊獲取請求和第一認證資訊發送至安全資訊應用，獲取安全資訊應用在對所述第一認證資訊認證通過後返回的簽名後的標準資訊以及標準資訊的身份標識，其中，所述簽名後的標準資訊是所述安全資訊應用使用第二認證資訊進行簽名的，將簽名後的標準資訊、所述標準資訊的身份標識以及所述第一認證資訊發送給所述認證伺服器，以使得所述認證伺服器在對所述第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將所述標準資訊和所述標準資訊的身份標識進行註冊。

【英文】

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

申請專利範圍

1. 一種資訊註冊方法，其特徵在於，該方法包括：

向認證伺服器發送標準資訊註冊請求；

接收該認證伺服器回饋的第一認證資訊；

生成標準資訊獲取請求，將該標準資訊獲取請求和該第一認證資訊發送至安全資訊應用，獲取該安全資訊應用在對該第一認證資訊認證通過後返回的簽名後的標準資訊以及該標準資訊的身份標識，其中，該簽名後的標準資訊是該安全資訊應用使用第二認證資訊進行簽名的；

將簽名後的標準資訊、該標準資訊的身份標識以及該第一認證資訊發送給該認證伺服器，以使得該認證伺服器在對該第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將該標準資訊和該標準資訊的身份標識進行註冊。

2. 如申請專利範圍第 1 項所述的方法，其中，接收該認證伺服器回饋的第一認證資訊，具體包括：

接收該認證伺服器發送的、採用該認證伺服器自身的第一加密密鑰進行簽名後的證書，並將簽名後的證書作為該第一認證資訊。

3. 一種資訊註冊方法，其特徵在於，該方法包括：

接收業務應用發送的第一認證資訊和標準資訊獲取請求；

對該第一認證資訊進行認證，並在認證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及該標準資訊

的身份標識返回給該業務應用，使該業務應用將簽名後的標準資訊以及該標準資訊的身份標識發送給認證伺服器，以使得該認證伺服器在對該第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將該標準資訊和該標準資訊的身份標識進行註冊。

4. 如申請專利範圍第 3 項所述的方法，其中，將使用第二認證資訊進行簽名後的標準資訊，以及該標準資訊的身份標識返回給該業務應用，具體包括：

接收用戶輸入的標準資訊；

使用第二認證資訊對該標準資訊進行簽名，並針對該標準資訊，確定該標準資訊的身份標識；

將簽名後的標準資訊以及該標準資訊的身份標識，返回給該業務應用。

5. 如申請專利範圍第 4 項所述的方法，其中，該標準資訊的身份標識，包括該標準資訊的身份密鑰資訊，該身份密鑰資訊與該用戶的帳戶資訊相關聯。

6. 如申請專利範圍第 3 項所述的方法，其中，該第一認證資訊中包括認證伺服器簽名後的證書；

對該第一認證資訊進行認證，具體包括：

使用與該認證伺服器的第一加密密鑰相匹配的第一解密密鑰對該簽名後的證書進行解密認證。

7. 如申請專利範圍第 4 項所述的方法，其中，該第二認證資訊包括預先與認證伺服器約定的第二密鑰資訊；其中，該第二密鑰資訊中包括第二加密密鑰和第二解密密

鑰；

使用第二認證資訊對該標準資訊進行簽名，具體包括：

針對該標準資訊，使用預先與認證伺服器約定的第二加密密鑰進行簽名。

8. 一種資訊註冊方法，其特徵在於，該方法包括：

認證伺服器接收業務應用發送的標準資訊註冊請求；

根據該標準資訊註冊請求，生成第一認證資訊並回饋給該業務應用；

接收該業務應用發送的簽名後的標準資訊、該標準資訊的身份標識以及該第一認證資訊；其中，該簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給該業務應用的；

對該第一認證資訊進行認證，並根據簽名後的標準資訊對該第二認證資訊進行認證；

在對該第一認證資訊和該第二認證資訊認證均通過後，將該標準資訊以及該標準資訊的身份標識進行註冊。

9. 如申請專利範圍第 8 項所述的方法，其中，根據該標準資訊註冊請求，生成第一認證資訊並回饋給該業務應用，具體包括：

根據該標準資訊註冊請求，調取該認證伺服器自身的證書；

使用自身的第一加密密鑰對該證書進行簽名，作為第一認證資訊，並回饋給該業務應用。

10. 如申請專利範圍第 8 項所述的方法，其中，對該第一認證資訊進行認證，具體包括：

使用第一解密密鑰對該第一認證資訊進行解密認證。

11. 如申請專利範圍第 8 項所述的方法，其中，該第二認證資訊包括預先由該認證伺服器與該安全資訊應用約定的第二密鑰資訊；其中，該第二密鑰資訊包括：第二加密密鑰和第二解密密鑰；簽名後的標準資訊是由該安全應用使用第二加密密鑰進行簽名的；

根據簽名後的標準資訊對該第二認證資訊進行認證，具體包括：

根據預先約定的第二密鑰資訊，使用與該安全資訊應用預先約定的第二解密密鑰，對簽名後的標準資訊進行解密，以便對該第二認證資訊進行認證。

12. 一種資訊認證方法，其特徵在於，該方法包括：

向認證伺服器發送針對待認證資訊的校驗請求；

接收該認證伺服器回饋的第一認證資訊；

生成待認證資訊獲取請求，將該待認證資訊獲取請求和該第一認證資訊發送至安全資訊應用，獲取該安全資訊應用在對該第一認證資訊認證通過後返回的待認證資訊以及該待認證資訊的待認證身份標識；

將該待認證資訊、該待認證身份標識以及該第一認證資訊發送給該認證伺服器，以使得該認證伺服器對該第一認證資訊、該待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給該業務應用。

13. 一種資訊認證方法，其特徵在於，該方法包括：
接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求；

對該第一認證資訊進行認證，並在認證通過後，將待認證資訊以及該待認證資訊的身份標識透過該業務應用發送至認證伺服器，以使得該認證伺服器對該第一認證資訊、該待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給該業務應用。

14. 如申請專利範圍第 13 項所述的方法，其中，根據攜帶有第一認證資訊的標準資訊獲取請求，將待認證資訊以及該待認證資訊的身份標識返回給該業務應用，具體包括：

對該標準資訊獲取請求中攜帶的該第一認證資訊進行認證；

在認證通過後，接收用戶輸入的待認證資訊；

識別該待認證資訊所屬的標準資訊，將與該標準資訊相匹配的身份標準確定為該待認證資訊的待認證身份標識；

將該待認證資訊以及該待認證資訊的待認證身份標識返回給該業務應用。

15. 一種資訊認證方法，其特徵在於，該方法包括：
認證伺服器接收業務應用發送的針對待認證資訊的校驗請求；

根據該校驗請求，生成第一認證資訊並回饋給該業務

應用；

接收該業務應用發送的待認證資訊、該待認證資訊的待認證身份標識以及該第一認證資訊；

分別對該第一認證資訊、該待認證身份標識以及該待認證資訊進行認證，生成認證結果回饋給該業務應用。

16. 如申請專利範圍第 15 項所述的方法，其中，分別對該第一認證資訊、該身份標識以及該待認證資訊進行認證，具體包括：

針對該第一認證資訊，使用自身的第一解密密鑰對該第一認證資訊進行解密，對解密後的該證書進行認證；

針對該待認證身份標識，根據已註冊的標準資訊的身份標識，判斷該待認證身份標識是否與已註冊的標識資訊的身份標識相匹配；

針對該待認證資訊，與已註冊的標準資訊進行比對認證。

17. 如申請專利範圍第 16 項所述的方法，其中，生成認證結果回饋給該業務應用，具體包括：

針對該第一認證資訊，若認證通過，則對該待認證資訊及待認證身份標識進行認證；否則，返回認證失敗通知；

針對該身份標識，若認證通過，則對該待認證資訊進行認證；否則，返回認證失敗通知；

針對該待認證資訊，若認證成功，則返回成功通知；否則，則返回認證失敗通知。

18. 一種資訊註冊裝置，其特徵在於，該裝置包括：
註冊請求模組，用於向認證伺服器發送標準資訊註冊請求；

接收模組，用於接收該認證伺服器回饋的第一認證資訊；

獲取模組，用於生成標準資訊獲取請求，將該標準資訊獲取請求和該第一認證資訊發送至安全資訊應用，獲取該安全資訊應用在對該第一認證資訊認證通過後返回的簽名後的標準資訊以及該標準資訊的身份標識，其中，該簽名後的標準資訊是該安全資訊應用使用第二認證資訊進行簽名的；

發送模組，用於將簽名後的標準資訊、該標準資訊的身份標識以及該第一認證資訊發送給該認證伺服器，以使得該認證伺服器在對該第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將該標準資訊和該標準資訊的身份標識進行註冊。

19. 如申請專利範圍第 18 項所述的裝置，其中，該接收模組，具體用於接收該認證伺服器發送的、採用該認證伺服器自身的第一加密密鑰進行簽名後的證書，並將簽名後的證書作為該第一認證資訊。

20. 一種資訊註冊裝置，其特徵在於，該裝置包括：
接收模組，用於接收業務應用發送的第一認證資訊和標準資訊獲取請求；

簽名模組，用於對該第一認證資訊進行認證，並在認

證通過後，將使用第二認證資訊進行簽名後的標準資訊，以及該標準資訊的身份標識返回給該業務應用，使該業務應用將簽名後的標準資訊以及該標準資訊的身份標識發送給認證伺服器，以使得該認證伺服器在對該第一認證資訊認證通過，且根據簽名後的標準資訊對第二認證資訊認證通過後，將該標準資訊和該標準資訊的身份標識進行註冊。

21. 如申請專利範圍第 20 項所述的裝置，其中，該簽名模組，具體用於接收用戶輸入的標準資訊，使用第二認證資訊對該標準資訊進行簽名，並針對該標準資訊，確定該標準資訊的身份標識，將簽名後的標準資訊以及該標準資訊的身份標識，返回給該業務應用。

22. 如申請專利範圍第 21 項所述的裝置，其中，該標準資訊的身份標識，包括該標準資訊的身份密鑰資訊，該身份密鑰資訊與該用戶的帳戶資訊相關聯。

23. 如申請專利範圍第 20 項所述的裝置，其中，該第一認證資訊中包括認證伺服器簽名後的證書；該簽名模組，具體用於使用與該認證伺服器的第一加密密鑰相匹配的第一解密密鑰對該簽名後的證書進行解密認證。

24. 如申請專利範圍第 21 項所述的裝置，其中，該第二認證資訊包括預先與認證伺服器約定的第二密鑰資訊；其中，該第二密鑰資訊中包括第二加密密鑰和第二解密密鑰；

該簽名模組，具體用於針對該標準資訊，使用預先與

認證伺服器約定的第二加密密鑰進行簽名。

25. 一種資訊註冊裝置，其特徵在於，該裝置包括：

註冊請求接收模組，用於接收業務應用發送的標準資訊註冊請求；

回饋模組，用於根據該標準資訊註冊請求，生成第一認證資訊並回饋給該業務應用；

註冊資訊接收模組，用於接收該業務應用發送的簽名後的標準資訊、該標準資訊的身份標識以及該第一認證資訊；其中，該簽名後的標準資訊是安全資訊應用使用第二認證資訊進行簽名，並發送給該業務應用的；

認證模組，用於對該第一認證資訊進行認證，並根據簽名後的標準資訊對該第二認證資訊進行認證；

註冊模組，用於在對該第一認證資訊和該第二認證資訊認證均通過後，將該標準資訊以及該標準資訊的身份標識進行註冊。

26. 如申請專利範圍第 25 項所述的裝置，其中，該回饋模組，具體用於根據該標準資訊註冊請求，調取該認證伺服器自身的證書，使用自身的第一加密密鑰對該證書進行簽名，作為第一認證資訊，並回饋給該業務應用。

27. 如申請專利範圍第 25 項所述的裝置，其中，該認證模組，具體用於使用第一解密密鑰對該第一認證資訊進行解密認證。

28. 如申請專利範圍第 25 項所述的裝置，其中，該第二認證資訊包括預先由該認證伺服器與該安全資訊應用

約定的第二密鑰資訊；其中，該第二密鑰資訊包括：第二加密密鑰和第二解密密鑰；簽名後的標準資訊是由該安全應用使用第二加密密鑰進行簽名的；

該認證模組，具體用於根據預先約定的第二密鑰資訊，使用與該安全資訊應用預先約定的第二解密密鑰，對簽名後的標準資訊進行解密，以便對該第二認證資訊進行認證。

29. 一種資訊認證裝置，其特徵在於，該裝置包括：

註冊請求模組，用於向認證伺服器發送針對待認證資訊的校驗請求；

接收模組，用於接收該認證伺服器回饋的第一認證資訊；

獲取模組，用於生成待認證資訊獲取請求，將該待認證資訊獲取請求和該第一認證資訊發送至安全資訊應用，獲取該安全資訊應用在對該第一認證資訊認證通過後返回的待認證資訊以及該待認證資訊的待認證身份標識；

發送模組，用於將該待認證資訊、該待認證身份標識以及該第一認證資訊發送給該認證伺服器，以使得該認證伺服器對該第一認證資訊、該待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給該業務應用。

30. 一種資訊認證裝置，其特徵在於，該裝置包括：

接收模組，用於接收業務應用發送的、攜帶有第一認證資訊的待認證資訊獲取請求；

簽名模組，用於對該第一認證資訊進行認證，並在認

證通過後，將待認證資訊以及該待認證資訊的身份標識透過該業務應用發送至認證伺服器，以使得該認證伺服器對該第一認證資訊、該待認證身份標識以及待認證資訊進行認證，生成認證結果回饋給該業務應用。

31. 如申請專利範圍第 30 項所述的裝置，其中，該簽名模組，具體用於對該標準資訊獲取請求中攜帶的該第一認證資訊進行認證，在認證通過後，識別該待認證資訊所屬的標準資訊，將與該標準資訊相匹配的身份標準確定為該待認證資訊的待認證身份標識，將該待認證資訊以及該待認證資訊的待認證身份標識返回給該業務應用。

32. 一種資訊認證裝置，其特徵在於，該裝置包括：

認證請求接收模組，用於接收業務應用發送的針對待認證資訊的校驗請求；

回饋模組，用於根據該校驗請求，生成第一認證資訊並回饋給該業務應用；

認證資訊接收模組，用於接收該業務應用發送的待認證資訊、該待認證資訊的待認證身份標識以及該第一認證資訊；

認證模組，用於分別對該第一認證資訊、該待認證身份標識以及該待認證資訊進行認證，生成認證結果回饋給該業務應用。

33. 如申請專利範圍第 32 項所述的裝置，其中，該認證模組，具體用於針對該第一認證資訊，使用自身的第一解密密鑰對該第一認證資訊進行解密，對解密後的該證

書進行認證；針對該待認證身份標識，根據已註冊的標準資訊的身份標識，判斷該待認證身份標識是否與已註冊的標識資訊的身份標識相匹配；針對該待認證資訊，與已註冊的標準資訊進行比對認證。

34. 如申請專利範圍第 33 項所述的裝置，其中，該認證模組，具體用於針對該第一認證資訊，若認證通過，則對該待認證資訊及待認證身份標識進行認證；否則，返回認證失敗通知；針對該身份標識，若認證通過，則對該待認證資訊進行認證；否則，返回認證失敗通知；針對該待認證資訊，若認證成功，則返回成功通知；否則，則返回認證失敗通知。

圖 式

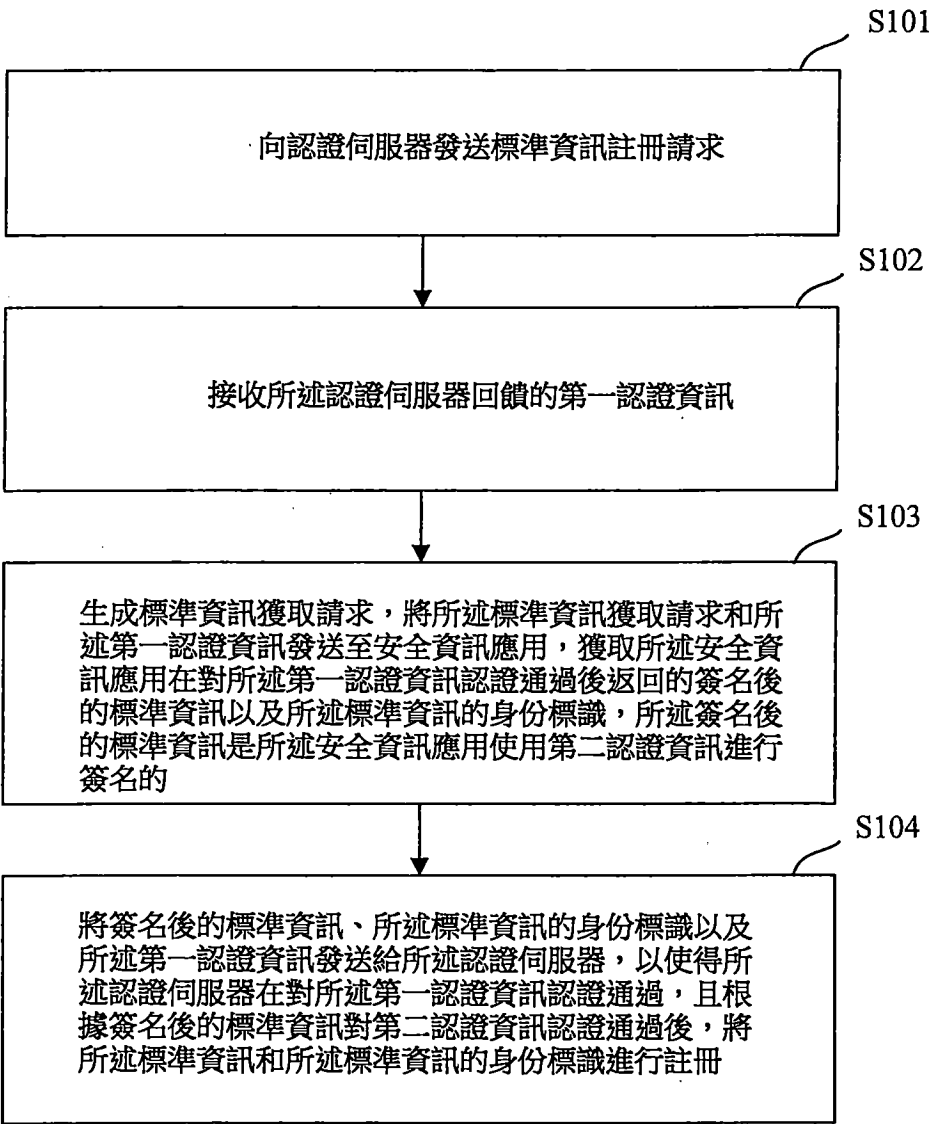


圖 1

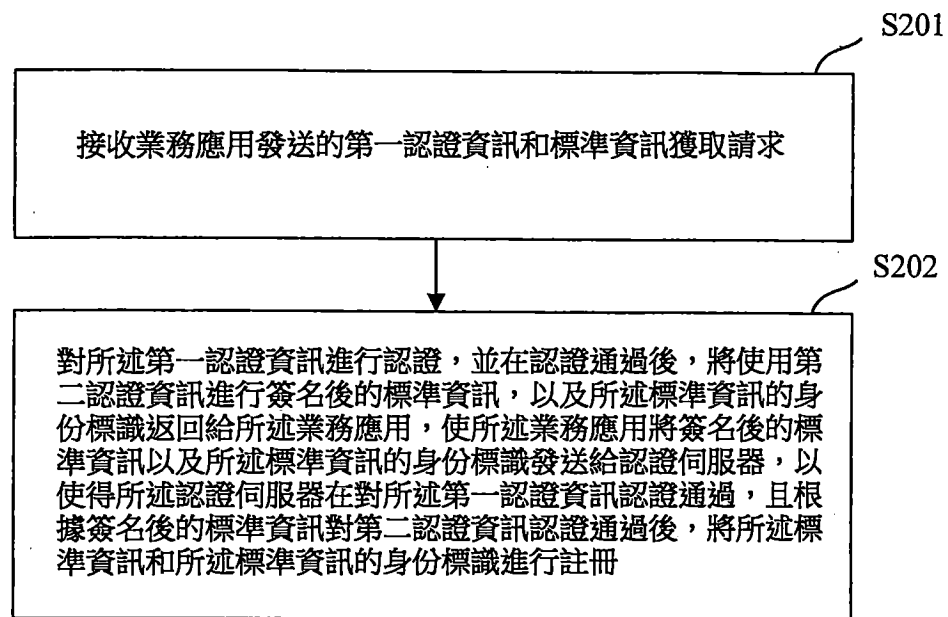


圖 2

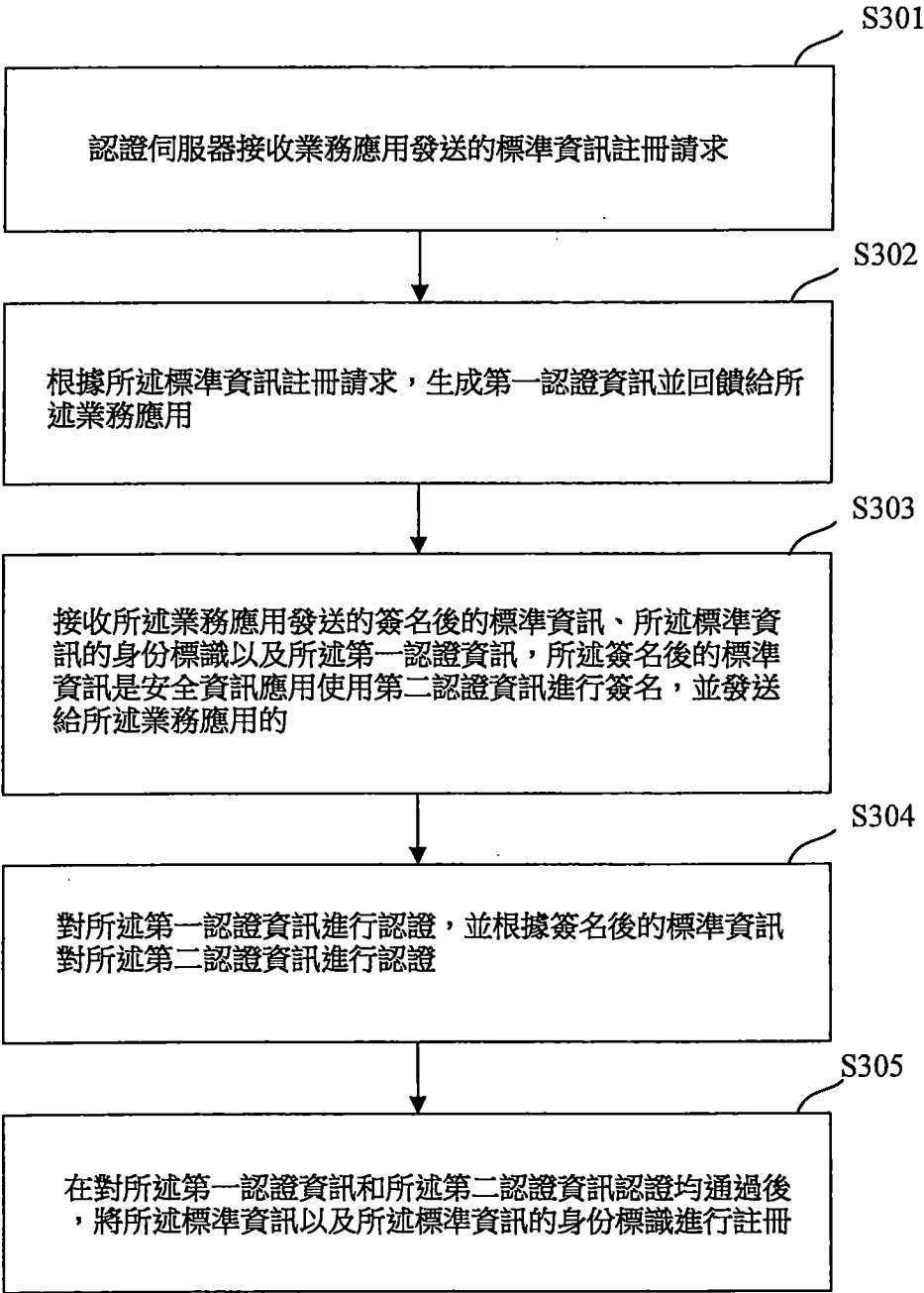


圖 3

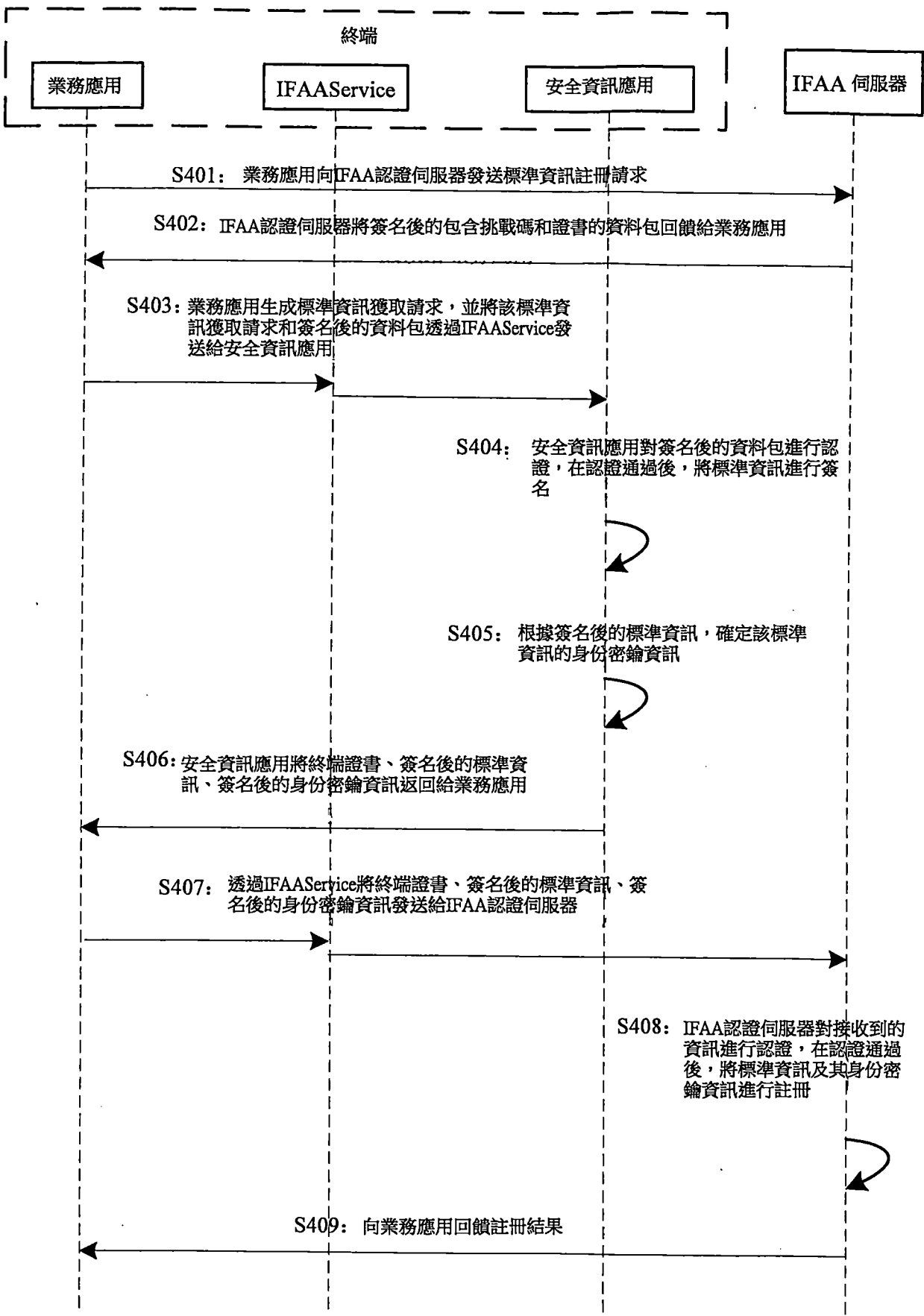


圖 4

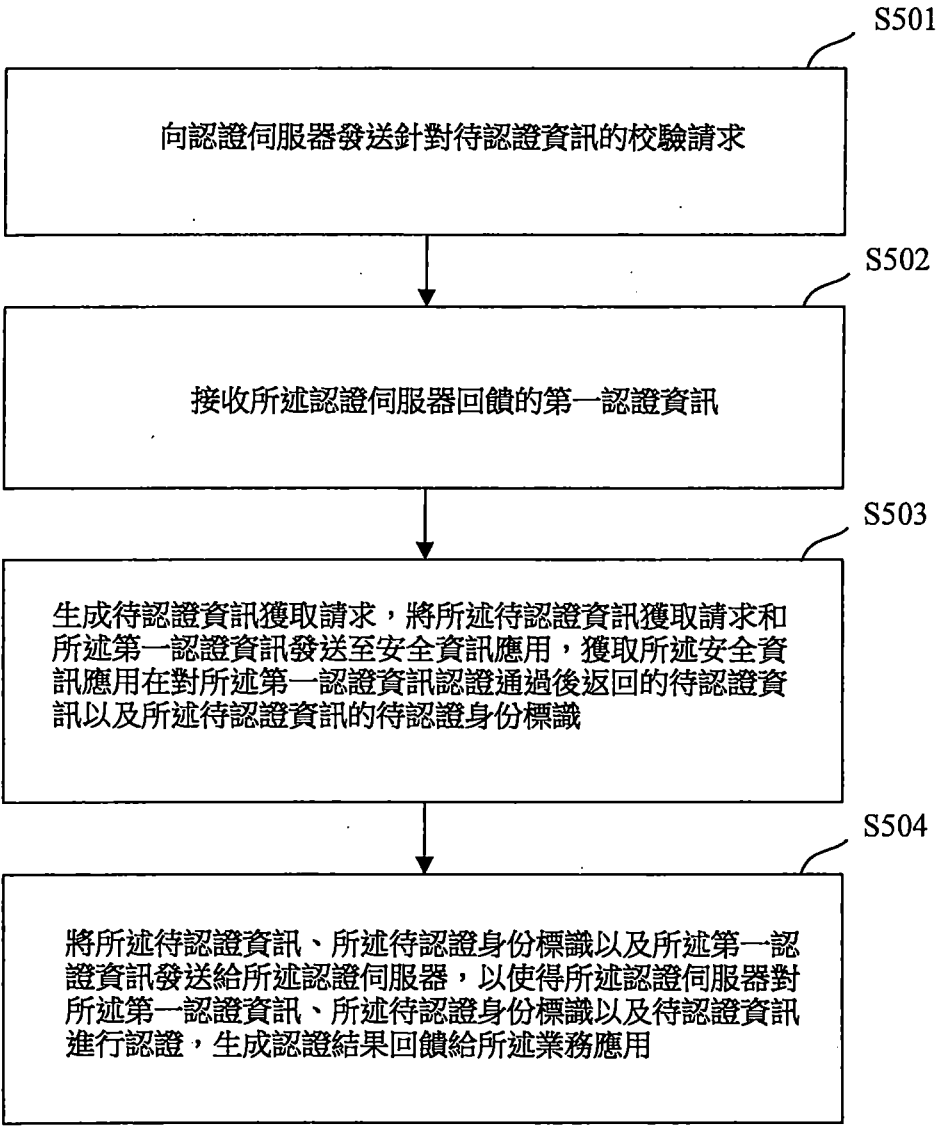


圖 5

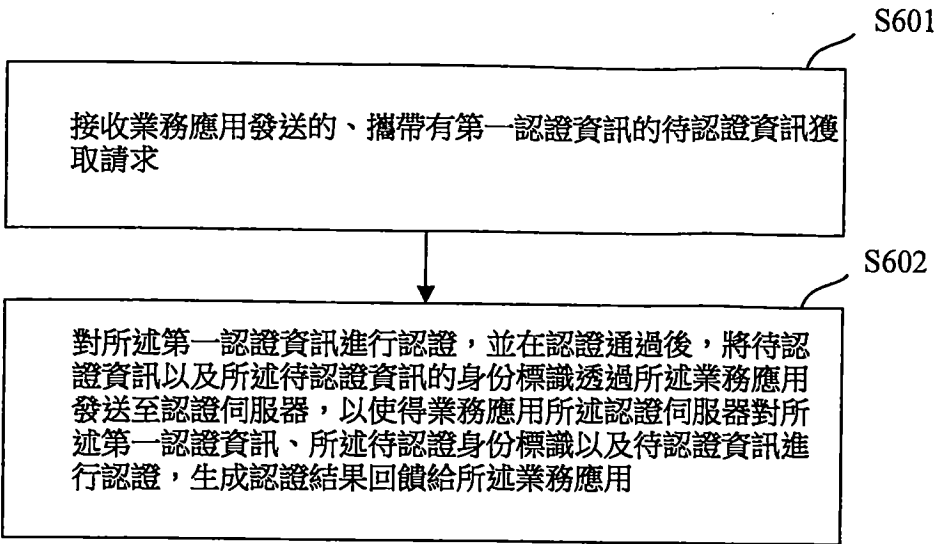


圖 6

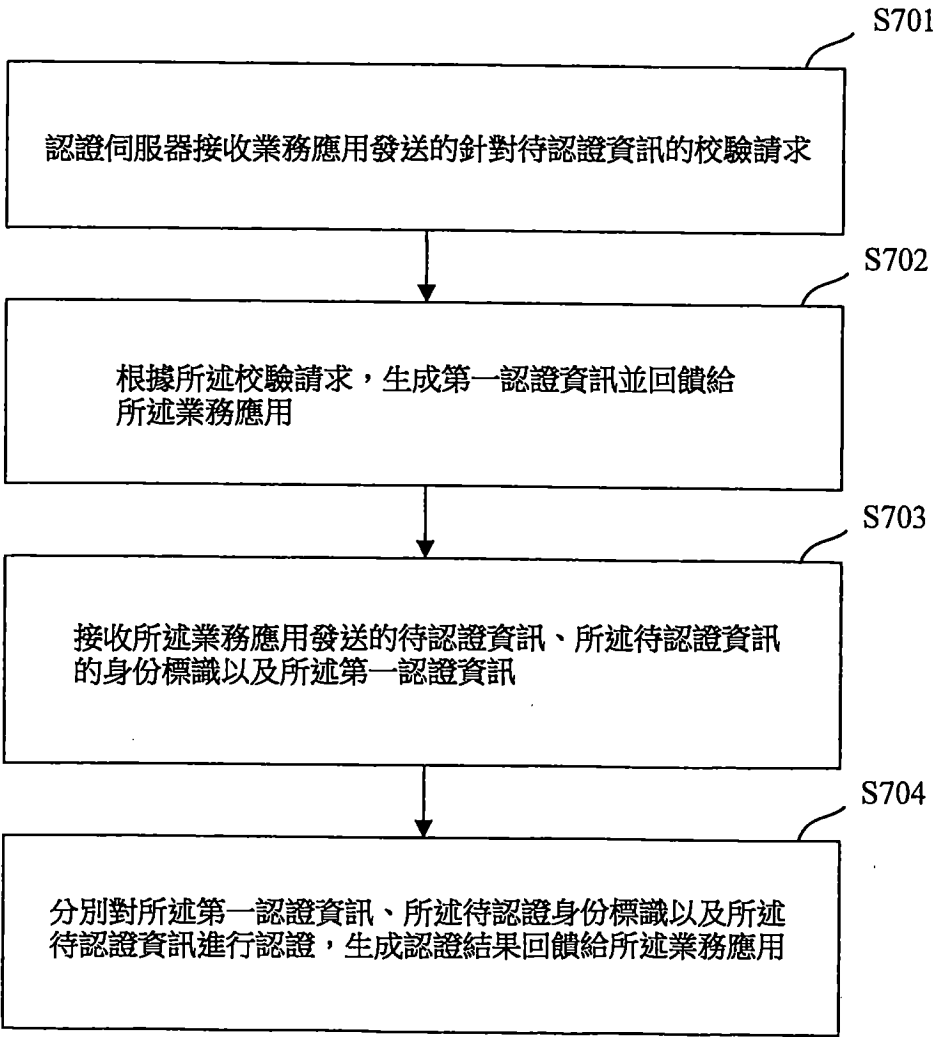


圖 7

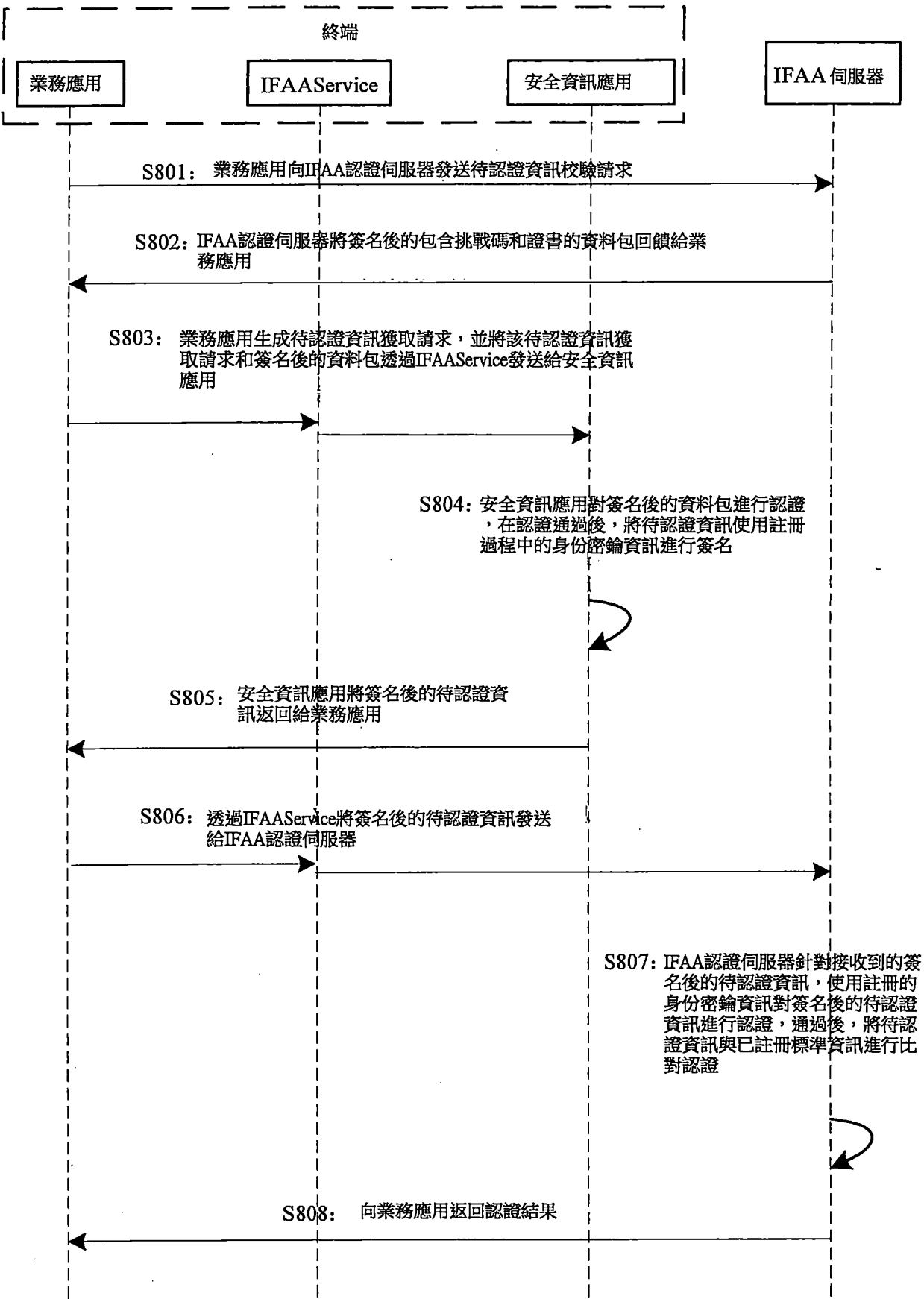


圖 8

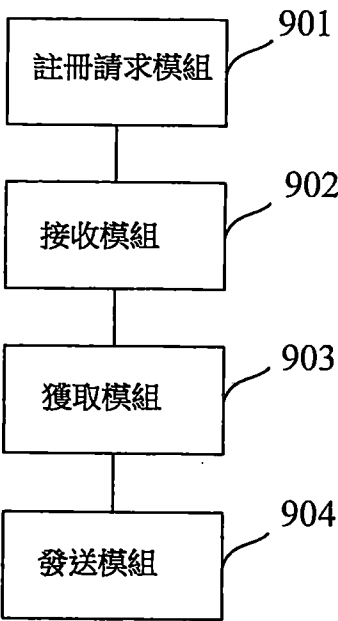


圖 9

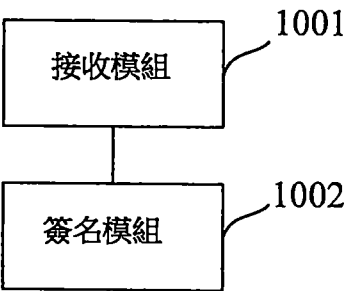


圖 10

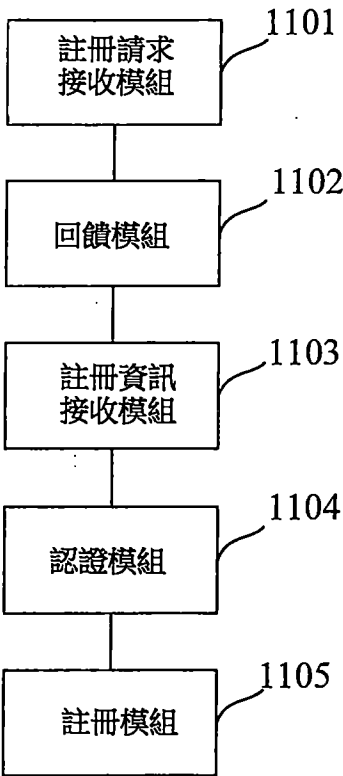


圖 11

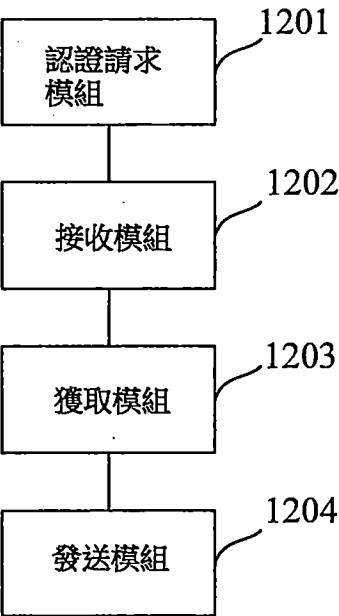


圖 12

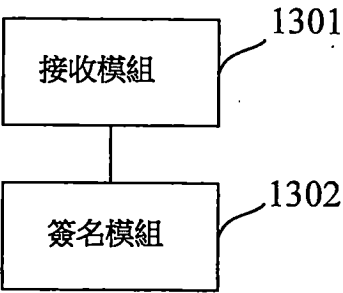


圖 13

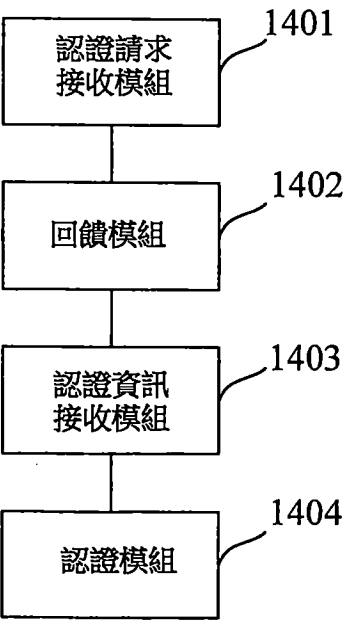


圖 14