



(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 I678909 B

(45)公告日：中華民國 108(2019)年 12 月 01 日

(21)申請案號：105107218

(22)申請日：中華民國 105(2016)年 03 月 09 日

(51)Int. Cl. : H04L9/32 (2006.01)

(30)優先權：2015/08/14 中國大陸 201510497438.X

(71)申請人：香港商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：郭棟 (CN)；鄧超 (CN)；陳廷梁 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 101051907A US 2012/0167186A1

US 2013/0205136A1 US 2014/0129430A1

US 2014/0344580A1 WO 2015/188538A1

審查人員：程敦睿

申請專利範圍項數：12 項 圖式數：6 共 36 頁

(54)名稱

安全認證方法、裝置及系統

(57)摘要

本發明提供一種安全認證方法、裝置及系統。在方法中，服務調用方預先獲得認證所需的符記並將符記儲存於本地，當需要調用應用平臺提供的服務時，根據本地預存的符記生成第一簽名，將第一簽名以及該服務調用方的標識添加到服務調用請求中發送給應用平臺；應用平臺根據服務調用請求中的第一簽名和服務調用方的標識，針對該服務調用請求進行安全認證。本發明可以使服務調用方在不登錄應用平臺(即非登錄狀態)下進行安全認證。

指定代表圖：

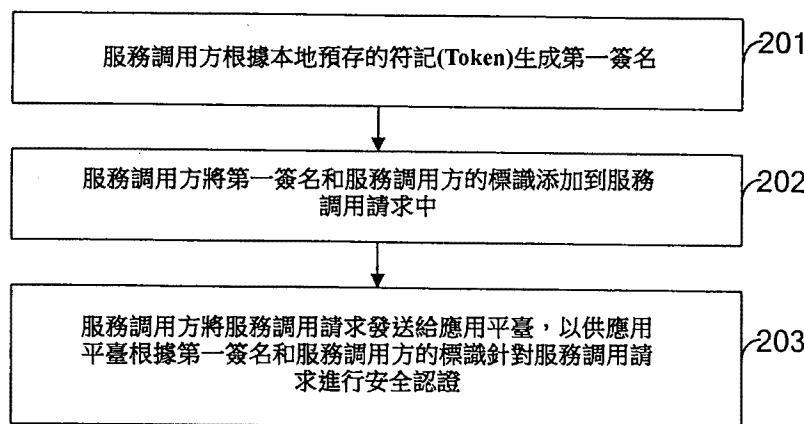


圖 2

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)

安全認證方法、裝置及系統

【技術領域】

本發明涉及網際網路技術領域，尤其涉及一種安全認證方法、裝置及系統。

【先前技術】

在當前雲端計算和大數據背景下，資料提供者、服務開發者以及服務使用者在基於大數據的應用平臺上的資料存取，資料交換，資料提交，服務二次開發等需求越來越多，這使得如何保證應用平臺的安全成為非常重要的問題。

目前業界已經有一些基於符記（token）的身分認證系統，但是這類系統大都基於對話（Session）或者網路餅乾（Cookie），是以用戶登錄為前提的身分驗證方法。但是，對於基於大數據的應用平臺來說，使用者需要在非登錄狀態下去調用應用平臺提供的服務，由此可見，應用平臺無法基於 Session 或 Cookie 進行安全認證。

【發明內容】

本發明的多個方面提供一種安全認證方法及裝置，用

以在非登錄狀態下實現安全認證，提高應用平臺的安全性。

本發明的一方面，提供一種安全認證方法，包括：

服務調用方根據本地預存的符記生成第一簽名；

所述服務調用方將所述第一簽名和所述服務調用方的標識添加到服務調用請求中；

所述服務調用方將所述服務調用請求發送給應用平臺，以供所述應用平臺根據所述第一簽名和所述服務調用方的標識針對所述服務調用請求進行安全認證。

本發明的另一方面，提供一種安全認證方法，包括：

應用平臺接收服務調用方發送的服務調用請求，所述服務調用請求包括所述服務調用方根據本地預存的符記生成的第一簽名和所述服務調用方的標識；

所述應用平臺根據所述第一簽名和所述服務調用方的標識，針對所述服務調用請求進行安全認證。

本發明的又一方面，提供一種安全認證裝置，於服務調用方實現，所述裝置包括：

生成模組，用於根據本地預存的符記生成第一簽名；

添加模組，用於將所述第一簽名和所述服務調用方的標識添加到服務調用請求中；

發送模組，用於將所述服務調用請求發送給應用平臺，以供所述應用平臺根據所述第一簽名和所述服務調用方的標識針對所述服務調用請求進行安全認證。

本發明的又一方面，提供一種安全認證裝置，位於符

記管理系統中實現，所述裝置包括：

接收模組，用於接收應用平臺發送的服務調用請求，所述服務調用請求包括服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的第一簽名、所述服務調用方的標識、所述服務參數和所述時間戳記；

獲取模組，用於根據所述服務調用方的標識，獲取所述服務調用方的符記；

生成模組，用於根據所述服務調用方的符記、所述服務參數和所述時間戳記生成第二簽名；

判斷模組，用於判斷所述第一簽名與所述第二簽名是否相同，並判斷所述時間戳記是否在有效期內；

發送模組，用於在所述第一簽名和所述第二簽名相同，且所述時間戳記在有效期內時，向所述應用平臺返回指示安全認證通過的認證結果資訊，或者在所述第一簽名和所述第二簽名不相同，或者所述時間戳記未在有效期內時，向所述應用平臺返回指示安全認證未通過的認證結果資訊。

本發明的又一方面，提供一種安全認證系統，包括：服務調用方和應用平臺；

所述服務調用方，用於根據本地預存的符記生成第一簽名，將所述第一簽名和所述服務調用方的標識添加到服務調用請求中，將所述服務調用請求發送給所述應用平臺；

所述應用平臺，用於接收所述服務調用請求，根據所述第一簽名和所述服務調用方的標識，針對所述服務調用請求進行安全認證。

在本發明中，服務調用方預先獲得認證所需的符記並將符記儲存於本地，當需要調用應用平臺提供的服務時，根據本地預存的符記生成第一簽名，將第一簽名以及該服務調用方的標識添加到服務調用請求中發送給應用平臺；應用平臺根據服務調用請求中的第一簽名和服務調用方的標識，針對該服務調用請求進行安全認證。由於服務調用方預先獲得符記並儲存在本地，所以不需要透過登錄應用平臺獲得認證所需的符記，使得服務調用方在不登錄應用平臺（即非登錄狀態）下也能夠進行安全認證。

【圖式簡單說明】

為了更清楚地說明本發明實施例中的技術方案，下面將對實施例或現有技術描述中所需要使用的圖式作一簡單地介紹，顯而易見地，下面描述中的圖式是本發明的一些實施例，對於本領域具有通常知識者來講，在不付出創造性勞動性的前提下，還可以根據這些圖式獲得其他的圖式。

圖 1 為本發明一實施例提供的安全認證系統的結構示意圖；

圖 2 為本發明一實施例提供的安全認證方法的流程示意圖；



圖 3 為本發明另一實施例提供的安全認證方法的流程示意圖；

圖 4 為本發明一實施例提供的安全認證裝置的結構示意圖；

圖 5 為本發明另一實施例提供的安全認證裝置的結構示意圖；

圖 6 為本發明又一實施例提供的安全認證裝置的結構示意圖。

【實施方式】

為使本發明實施例的目的、技術方案和優點更加清楚，下面將結合本發明實施例中的圖式，對本發明實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例是本發明一部分實施例，而不是全部的實施例。基於本發明中的實施例，本領域具有通常知識者在沒有作出創造性勞動前提下所獲得的所有其他實施例，都屬於本發明保護的範圍。

針對現有技術存在的無法在非登錄狀態下進行安全認證的問題，本發明提供一種解決方案，其主要原理是：服務調用方預先獲得認證所需的符記並將其儲存在本地，當需要調用應用平臺提供的服務時，直接根據本地預存的符記生成認證使用的簽名，將簽名和服務調用方的標識添加到服務調用請求中發送給應用平臺，使得應用平臺能夠根據調用服務請求中的簽名和服務調用方的標識針對該服務

調用請求進行安全認證。由此可見，服務調用方可以在不用登錄應用平臺的情況下可以向應用平臺發起認證，解決了非登錄狀態下無法進行安全認證的問題。

本發明提供的技術方案可由安全認證系統來執行。如圖 1 所示，該安全認證系統包括：服務調用方 10 和應用平臺 20。

服務調用方 10 是指需要調用應用平臺 20 提供的服務的一方。應用平臺 20 主要負責提供各種各樣的服務，例如可以是基於大數據實現的應用平臺。所述大數據中的資料是指廣義概念上的資料，例如清單、使用者自訂函數 UDF、資料服務、報表等都屬於資料。

在應用平臺 20 內部，各種服務可以以業務模組的形式分散式部署在不同的位置。由於服務之間的聯繫，業務模組和業務模組之間需要相互調用。意味著，服務調用方 10 可以是來自應用平臺 20 內部的業務模組。在業務模組互動過程中，應用平臺 20 需要發起服務調用的業務模組進行安全認證，防止來自網路內部的非法請求。

另外，服務調用方 10 還可以是來自應用平臺 20 外部的網路使用者。由於應用平臺 20 外部的網路使用者可能來自公網的各種網路環境，請求調用服務的形式包括但不限於應用程式介面（API）調用，程式化腳本（shell script），UDF 任務等。因此，應用平臺 20 需要對來自應用平臺 20 外部的服務調用請求進行安全認證，確保請求是合法的。

考慮到服務調用方 10 可能不會登錄應用平臺 20，而是直接向應用平臺發起服務調用，於是需要在非登錄狀態下進行安全認證。具體的：

服務調用方 10 預先獲得認證使用的符記並儲存在本地。當需要調用應用平臺 20 提供的服務時，服務調用方 10 根據本地預存的符記（token）生成第一簽名；將第一簽名和服務調用方 10 的標識添加到服務調用請求中；將服務調用請求發送給應用平臺 20。應用平臺 20 接收服務調用方 10 發送的服務調用請求；根據服務調用請求中的第一簽名和服務調用方 10 的標識針對該服務調用請求進行安全認證。

舉例說明，若服務調用方 10 為應用平臺 20 外部的網路使用者，則應用平臺 20 可以透過設置租戶群體和專案對外部網路使用者進行管理。租戶是使用應用平臺 20 提供的資源和/或服務的客戶群，不同租戶具有不同的 id；專案是網路使用者在應用平臺 20 下對資料進行加工處理的場所，網路使用者可以按照不同的產品線劃分不同的專案使用。專案是網路使用者操作數據資源的基本單位，從屬於租戶，一個租戶下可以擁有多個專案，不同專案具有不同的 id。在該舉例中，服務調用方 10 的標識可以包括：用戶 id、租戶 id 和專案 id。

舉例說明，若服務調用方 10 為應用平臺 20 內部的業務模組，則應用平臺 20 可以統一管理各業務模組並為各業務模組分配 baseKey 作為業務模組的標識。在該舉例

中，服務調用方 10 的標識具體是指業務模組的標識，例如 baseKey。

在本系統中，由於服務調用方預先獲得符記並儲存在本地，所以不需要透過登錄應用平臺獲得認證所需的符記，使得服務調用方在不登錄應用平臺（即非登錄狀態）下也能夠進行安全認證。

進一步，如圖 1 所示，該安全認證系統還包括：符記（token）管理系統 30。

其中，應用平臺 20 具體透過將服務調用請求發送給符記管理系統 30，以供符記管理系統 30 進行安全認證，並接收符記管理系統 30 返回的認證結果資訊。

符記管理系統 30 主要根據服務調用請求中的第一簽名和服務調用方 10 的標識針對該服務調用請求進行安全認證。

例如，符記管理系統 30 管理服務調用方 10 與服務調用方 10 使用的符記之間的映射關係。則，符記管理系統 30 可以從服務調用請求中解析出服務調用方 10 的標識，根據服務調用方 10 的標識獲取服務調用方 10 的符記；基於獲取的符記生成第二簽名；將第一簽名和第二簽名進行比較，若兩個簽名相同，則確認安全認證通過，向應用平臺 20 返回指示安全認證通過的認證結果資訊；若兩個簽名不相同，則確認安全認證未通過，向應用平臺 20 返回指示安全認證未通過的認證結果資訊。

在一可選實施方式中，為了能夠針對每次服務調用請

求單獨進行安全認證，服務調用方 10 在生成第一簽名時除了使用本地預存的符記之外，還採用本次服務調用所需的服務參數和本機服務調用的時間戳記。由於不同服務調用的時間戳記不同，且不同服務調用所需的服務參數一般也會發生變化，所以透過本次服務調用所需的服務參數和本機服務調用的時間戳記能夠唯一標識一次服務請求，因此將符記與服務調用時所需的服務參數和時間戳記相結合進行安全認證能夠達到對每次服務調用進行單獨認證的效果，解決現有 SSO 模式無法針對每次服務調用進行單獨認證的問題。

具體的，服務調用方 10 根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成第一簽名，將第一簽名、服務調用方的標識、本次服務調用所需的服務參數和本次服務調用的時間戳記添加到服務調用請求中，發送給應用平臺 20。

可選的，一種生成第一簽名的方式如下：

將本次服務調用所需的服務參數和本次服務調用的時間戳記組合為調用參數，按照調用參數中的分隔符號（例如 &）對調用參數進行切分，以獲得多個參數段，並按照字元順序（例如可以是升冪）對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加上述符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫

字元，以獲得第一簽名。例如，可以對第二參數序列進行 SHA256 編碼，但不限於此。

值得說明的是，本實施例生成第一簽名的方式並不限於上述實施方式提供的方式，現有技術中各種生成簽名的方式也適用於本實施例。

應用平臺 20 接收服務調用方 10 發送的服務調用請求；將服務調用請求發送給符記管理系統 30，接收符記管理系統 30 返回的認證結果資訊。如果認證結果資訊指示安全認證通過，應用平臺 20 按服務功能向服務調用方 10 提供相應的服務；否則，應用平臺 20 直接拒絕服務調用方 10 此次的服務調用請求。

符記管理系統 30 接收應用平臺 20 發送的服務調用請求；根據服務調用請求中服務調用方 10 的標識，獲取服務調用方 10 的符記，根據服務調用方 10 的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成第二簽名，判斷第一簽名與第二簽名是否相同，並判斷本次服務調用的時間戳記是否在有效期內；若第一簽名和第二簽名相同，且本次服務調用的時間戳記在有效期內，向應用平臺 20 返回指示安全認證通過的認證結果資訊；若第一簽名和第二簽名不相同，或者本次服務調用的時間戳記未在有效期內，向應用平臺 20 返回指示安全認證未通過的認證結果資訊。

可選的，一種生成第二簽名的方式如下：

將本次服務調用所需的服務參數和本次服務調用的時

間戳記組合為調用參數，按照調用參數中的分隔符號（例如 &）對調用參數進行切分，以獲得多個參數段，並按照字元順序（例如可以是升冪）對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加上述符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得第二簽名。例如，可以對第二參數序列進行 SHA256 編碼，但不限於此。

值得說明的是，本實施例生成第二簽名的方式並不限於上述實施方式提供的方式，現有技術中各種生成簽名的方式也適用於本實施例。

但是，在同一安全認證過程中，服務調用方生成第一簽名的方式與符記管理系統 30 生成第二簽名的方式必須是一致的。

可選的，符記管理系統 30 判斷本次服務調用的時間戳記是否在有效期內的一種實施方式為：比較符記管理系統 30 的時間和服務調用請求中攜帶的時間戳記的差值是否超過了預設的實效門檻，如果兩者的差值超過了失效門檻，則認為本次服務調用的時間戳記未在有效期內；如果兩者的差值未超過失效門檻，則認為本次服務調用的時間戳記在有效期內。

進一步，符記管理系統 30 還負責預先為服務調用方 10 生成符記。則服務調用方 10 根據本地預存的符記生成

第一簽名之前，向符記管理系統 30 申請符記，並將申請到的符記儲存在本地。

具體的，服務調用方 10 向符記管理系統 30 發送符記申請請求，以申請符記；符記申請請求包括服務調用方的標識。符記管理系統 30 接收服務調用方 10 發送的符記申請請求；為服務調用方 10 生成符記；將生成的符記發送給服務調用方 10。服務調用方 10 接收符記管理系統 30 為服務調用方 10 生成的符記。

其中，符記管理系統 30 為服務調用方 10 生成符記的過程如下：

生成亂數；例如可以採用 SHA1PRNG 演算法生成亂數，但不限於 SHA1PRNG 演算法；

根據服務調用方 10 的標識和上述亂數構造原始串；例如，將服務調用方 10 的標識和上述亂數串接起來作為原始串；

對原始串進行編碼以生成符記。例如，可以對原始串進行 SHA256 編碼，但不限於此。

值得說明的是，本實施例生成符記的方式並不限於上述實施方式提供的方式，現有技術中各種生成符記的方式也適用於本實施例。

值得說明的是，上述系統中的應用平臺 20 與符記管理系統 30 可以獨立部署於不同的設備上實現，也可以部署於同一設備上實現。

從層次結構來說，本系統底層可以採用 hadoop、

spart、storm 等資料平臺，中間層可以採用開放的資料服務管理平臺，上層可以透過電腦程式設計語言和資料庫等構建資料管理和 web 系統。

本系統可以在非登錄態下對平臺外部的網路使用者或平臺內部的業務模組進行安全認證，並且可以對每一次服務調用請求進行單獨的安全認證和時效性控制，避免了請求的偽造和所有非法存取，保證了應用平臺的安全性。

以下實施例將分別從服務調用方和應用平臺的角度描述安全認證過程。

圖 2 為本發明一實施例提供的安全認證方法的流程示意圖。如圖 2 所示，該方法包括：

201、服務調用方根據本地預存的符記生成第一簽名。

202、服務調用方將第一簽名和服務調用方的標識添加到服務調用請求中。

203、服務調用方將服務調用請求發送給應用平臺，以供應用平臺根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證。

在本實施例中，服務調用方預先獲得認證所需的符記並將符記儲存於本地，當需要調用應用平臺提供的服務時，根據本地預存的符記生成認證所需的第一簽名，不需要透過登錄應用平臺獲得認證所需的符記，使得服務調用方在不登錄應用平臺（即非登錄狀態）下也能夠進行安全認證。

在一可選實施方式中，上述步驟 201 的實施過程包括：服務調用方根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成第一簽名。相應的，上述步驟 202 的實施過程包括：服務調用方將第一簽名、服務調用方的標識、本次服務調用所需的服務參數和本次服務調用的時間戳記添加到服務調用請求中。

進一步，服務調用方根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成第一簽名具體為：

將本次服務調用所需的服務參數和本次服務調用的時間戳記組合為調用參數，按照調用參數中的分隔符號（例如 &）對調用參數進行切分，以獲得多個參數段，並按照字元順序（例如可以是升冪）對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得第一簽名。例如，可以對第二參數序列進行 SHA256 編碼，但不限於此。

值得說明的是，本實施例生成第一簽名的方式並不限於上述實施方式提供的方式，現有技術中各種生成簽名的方式也適用於本實施例。

在該實施方式中，將符記與本次服務調用所需的服務參數和本機服務調用的時間戳記相結合生成第一簽名，並

在服務調用請求中同時攜帶第一簽名、本次服務調用所需的服務參數和本機服務調用的時間戳記，由於本次服務調用所需的服務參數和本機服務調用的時間戳記能夠唯一標識一次服務請求，因此將符記與服務調用時所需的服務參數和時間戳記相結合進行安全認證能夠達到對每次服務調用進行單獨認證的效果，解決現有 SSO 模式無法針對每次服務調用進行單獨認證的問題。

在一可選實施方式中，服務調用方可以在使用符記之前，向符記管理系統申請符記，並將申請到的符記儲存在本地。具體的，服務調用方向符記管理系統發送符記申請請求；接收符記管理系統發送的符記管理系統為服務調用方生成的符記。

除了向符記管理系統申請符記之外，符記管理系統也可以主動為服務調用方生成符記並下發給服務調用方。

其中，服務調用方為應用平臺內部的業務模組；或者服務調用方為應用平臺外部的網路使用者。

圖 3 為本發明另一實施例提供的安全認證方法的流程示意圖。如圖 3 所示，該方法包括：

301、應用平臺接收服務調用方發送的服務調用請求，服務調用請求包括服務調用方根據本地預存的符記生成的第一簽名和服務調用方的標識。

302、應用平臺根據第一簽名和服務調用方的標識，針對該服務調用請求進行安全認證。

在一可選實施方式中，上述步驟 202 具體為：應用平

臺將服務調用請求發送給符記管理系統，以供符記管理系統根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證；應用平臺接收符記管理系統返回的認證結果資訊。相應的，所述方法還包括：符記管理系統根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證的步驟。

在一可選實施方式中，第一簽名是服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的。相應的，服務調用請求還包括：本次服務調用所需的服務參數和本次服務調用的時間戳記。

基於此，上述符記管理系統根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證的過程具體為：

符記管理系統根據服務調用方的標識，獲取服務調用方的符記；

符記管理系統根據服務調用方的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成第二簽名；

符記管理系統判斷第一簽名與第二簽名是否相同，並判斷本次服務調用的時間戳記是否在有效期內；

若第一簽名和第二簽名相同，且本次服務調用的時間戳記在有效期內，符記管理系統向應用平臺返回指示安全認證通過的認證結果資訊；

若第一簽名和第二簽名不相同，或者本次服務調用的

時間戳記未在有效期內，符記管理系統向應用平臺返回指示安全認證未通過的認證結果資訊。

進一步，符記管理系統根據服務調用方的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成第二簽名，包括：

將本次服務調用所需的服務參數和本次服務調用的時間戳記組合為調用參數，按照調用參數中的分隔符號對調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得第二簽名。

值得說明的是，本實施例生成第二簽名的方式並不限於上述實施方式提供的方式，現有技術中各種生成簽名的方式也適用於本實施例。

進一步，所述方法在步驟 301 之前還包括以下步驟：

符記管理系統接收服務調用方發送的符記申請請求；

符記管理系統為服務調用方生成符記；

符記管理系統將符記發送給服務調用方。

其中，符記管理系統為服務調用方生成符記的實施過程為：

生成亂數；例如可以採用 SHA1PRNG 演算法生成亂數，但不限於 SHA1PRNG 演算法；

根據服務調用方的標識和亂數構造原始串；例如，將服務調用方 10 的標識和上述亂數串接起來作為原始串；

對原始串進行編碼以生成符記。例如，可以對原始串進行 SHA256 編碼，但不限於此。

值得說明的是，本實施例生成符記的方式並不限於上述實施方式提供的方式，現有技術中各種生成符記的方式也適用於本實施例。

可選的，上述服務調用方為應用平臺內部的業務模組；或者服務調用方為應用平臺外部的網路使用者。

在本實施例中，應用平臺與服務調用方相互配合，使得服務調用方能夠在不登錄應用平臺的情況下發起服務調用並進行安全認證，實現了非登錄狀態下的安全認證，解決了現有技術存在的問題。進一步，應用平臺與符記管理系統相結合，使得符記管理系統執行具體的認證流程，有利於減輕應用平臺的負擔。

需要說明的是，對於前述的各方法實施例，為了簡單描述，故將其都表述為一系列的動作組合，但是本領域具有通常知識者應該知悉，本發明並不受所描述的動作順序的限制，因為依據本發明，某些步驟可以採用其他順序或者同時進行。其次，本領域具有通常知識者也應該知悉，說明書中所描述的實施例均屬於較佳實施例，所涉及的動作和模組並不一定是本發明所必須的。

在上述實施例中，對各個實施例的描述都各有側重，某個實施例中沒有詳述的部分，可以參見其他實施例的相

關描述。

圖 4 為本發明一實施例提供的安全認證裝置的結構示意圖。該裝置於服務調用方實現，如圖 4 所示，該裝置包括：生成模組 41、添加模組 42 和發送模組 43。

生成模組 41，用於根據本地預存的符記生成第一簽名。

添加模組 42，用於將第一簽名和服務調用方的標識添加到服務調用請求中。

發送模組 43，用於將服務調用請求發送給應用平臺，以供應用平臺根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證。

在一可選實施方式中，生成模組 41 具體用於：

根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成第一簽名；

添加模組 42 具體用於：

將第一簽名、服務調用方的標識、服務參數和時間戳記添加到服務調用請求中。

進一步，生成模組 41 具體用於：

將服務參數和時間戳記組合為調用參數，按照調用參數中的分隔符號對調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得第一簽名。

在一可選實施方式中，安全認證裝置還包括：申請模組和儲存模組。

申請模組，用於向符記管理系統申請符記；

儲存模組，用於在本地儲存申請模組申請到的符記。

進一步，申請模組具體用於：

向符記管理系統發送符記申請請求；

接收符記管理系統發送的符記管理系統為服務調用方生成的符記。

值得說明的是，服務調用方為應用平臺內部的業務模組；或者服務調用方為應用平臺外部的網路使用者。

本實施例提供的安全認證裝置，於服務調用方實現，使得服務調用方能夠在不登錄應用平臺的情況下發起服務調用並進行安全認證，解決了現有技術在非登錄狀態下無法進行安全認證的問題。

圖 5 為本發明另一實施例提供的安全認證裝置的結構示意圖。該安全認證裝置位於應用平臺中實現，如圖 5 所示，該裝置包括：接收模組 51 和認證模組 52。

接收模組 51，用於接收服務調用方發送的服務調用請求，服務調用請求包括服務調用方根據本地預存的符記生成的第一簽名和服務調用方的標識。

認證模組 52，用於根據第一簽名和服務調用方的標識，針對服務調用請求進行安全認證。

可選的，認證模組 52 具體可用於：

將服務調用請求發送給符記管理系統，以供符記管理系統根據第一簽名和服務調用方的標識針對服務調用請求進行安全認證；

接收符記管理系統返回的認證結果資訊。

在一可選實施方式中，接收模組 51 接收到的服務調用請求還包括：本次服務調用所需的服務參數和本次服務調用的時間戳記；第一簽名是服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的。這樣可以實現對每次服務調用進行單獨安全認證，有利於請求的偽造和非法存取。

圖 6 為本發明又一實施例提供的安全認證裝置的結構示意圖。該安全認證裝置位於符記管理系統中實現，如圖 6 所示，該裝置包括：接收模組 61、獲取模組 62、生成模組 63、判斷模組 64 和發送模組 65。

接收模組 61，用於接收應用平臺發送的服務調用請求，服務調用請求包括服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的第一簽名、服務調用方的標識、服務參數和時間戳記。

獲取模組 62，用於根據服務調用方的標識，獲取服務調用方的符記。

生成模組 63，用於根據服務調用方的符記、服務參數和時間戳記生成第二簽名。

判斷模組 64，用於判斷第一簽名與第二簽名是否相同，並判斷時間戳記是否在有效期內。

發送模組 65，用於在第一簽名和第二簽名相同，且時間戳記在有效期內時，向應用平臺返回指示安全認證通過的認證結果資訊，或者在第一簽名和第二簽名不相同，或者時間戳記未在有效期內時，向應用平臺返回指示安全認證未通過的認證結果資訊。

在一可選實施方式中，生成模組 63 具體可用於：

將服務參數和時間戳記組合為調用參數，按照調用參數中的分隔符號對調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

在第一參數序列前端和後端分別添加符記，以獲得第二參數序列；

對第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得第二簽名。

在一可選實施方式中，接收模組 61 還用於：接收服務調用方發送的符記申請請求；相應的，生成模組 63 還用於：為服務調用方生成符記；發送模組 65 還用於：將符記發送給服務調用方。

生成模組 63 在為服務調用方生成符記時，具體用於：

生成亂數；

根據服務調用方的標識和亂數構造原始串；

對原始串進行編碼以生成符記。

本實施例提供的安全認證裝置，與上述實施例提供的安全認證裝置相配合，使得服務調用方能夠在非登錄狀態下進行服務調用和安全認證，解決了現有技術無法在非登錄狀態下進行安全認證的問題。

所屬領域的具有通常知識者可以清楚地瞭解到，為描述的方便和簡潔，上述描述的系統，裝置和單元的具體工作過程，可以參考前述方法實施例中的對應過程，在此不再贅述。

在本發明所提供的幾個實施例中，應該理解到，所揭露的系統，裝置和方法，可以透過其它的方式實現。例如，以上所描述的裝置實施例僅僅是示意性的，例如，所述單元的劃分，僅僅為一種邏輯功能劃分，實際實現時可以有另外的劃分方式，例如多個單元或元件可以結合或者可以集成到另一個系統，或一些特徵可以忽略，或不執行。另一點，所顯示或討論的相互之間的耦合或直接耦合或通訊連接可以是透過一些介面，裝置或單元的間接耦合或通訊連接，可以是電性，機械或其它的形式。

所述作為分離部件說明的單元可以是或者也可以不是物理上分開的，作為單元顯示的部件可以是或者也可以不是物理單元，即可以位於一個地方，或者也可以分佈到多個網路單元上。可以根據實際的需要選擇其中的部分或者全部單元來實現本實施例方案的目的。

另外，在本發明各個實施例中的各功能單元可以集成

在一個處理單元中，也可以是各個單元單獨物理存在，也可以兩個或兩個以上單元集成在一個單元中。上述集成的單元既可以採用硬體的形式實現，也可以採用硬體加軟體功能單元的形式實現。

上述以軟體功能單元的形式實現的集成的單元，可以儲存在一個電腦可讀取儲存介質中。上述軟體功能單元儲存在一個儲存介質中，包括若干指令用以使得一台電腦設備（可以是個人電腦，伺服器，或者網路設備等）或處理器（processor）執行本發明各個實施例所述方法的部分步驟。而前述的儲存介質包括：隨身碟、行動硬碟、唯讀記憶體（Read-Only Memory，ROM）、隨機存取記憶體（Random Access Memory，RAM）、磁碟或者光碟等各種可以儲存程式碼的介質。

最後應說明的是：以上實施例僅用以說明本發明的技術方案，而非對其限制；儘管參照前述實施例對本發明進行了詳細的說明，本領域的具有通常知識者應當理解：其依然可以對前述各實施例所記載的技術方案進行修改，或者對其中部分技術特徵進行等同替換；而這些修改或者替換，並不使相應技術方案的本質脫離本發明各實施例技術方案的精神和範圍。

【符號說明】

10：服務調用方

20：應用平臺

30：符記管理系統

201~203：步驟

301、302：步驟

41：生成模組

42：添加模組

43：發送模組

51：接收模組

52：認證模組

61：接收模組

62：獲取模組

63：生成模組

64：判斷模組

65：發送模組

公告本

I678909

發明摘要

※申請案號：105107218

※申請日：105 年 03 月 09 日 ※IPC 分類：

【發明名稱】(中文/英文)

安全認證方法、裝置及系統

【中文】

本發明提供一種安全認證方法、裝置及系統。在方法中，服務調用方預先獲得認證所需的符記並將符記儲存於本地，當需要調用應用平臺提供的服務時，根據本地預存的符記生成第一簽名，將第一簽名以及該服務調用方的標識添加到服務調用請求中發送給應用平臺；應用平臺根據服務調用請求中的第一簽名和服務調用方的標識，針對該服務調用請求進行安全認證。本發明可以使服務調用方在不登錄應用平臺（即非登錄狀態）下進行安全認證。

【英文】

【代表圖】

【本案指定代表圖】：第(2)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

圖 式

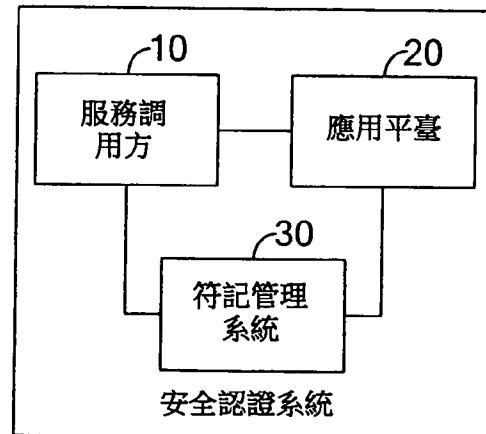


圖 1

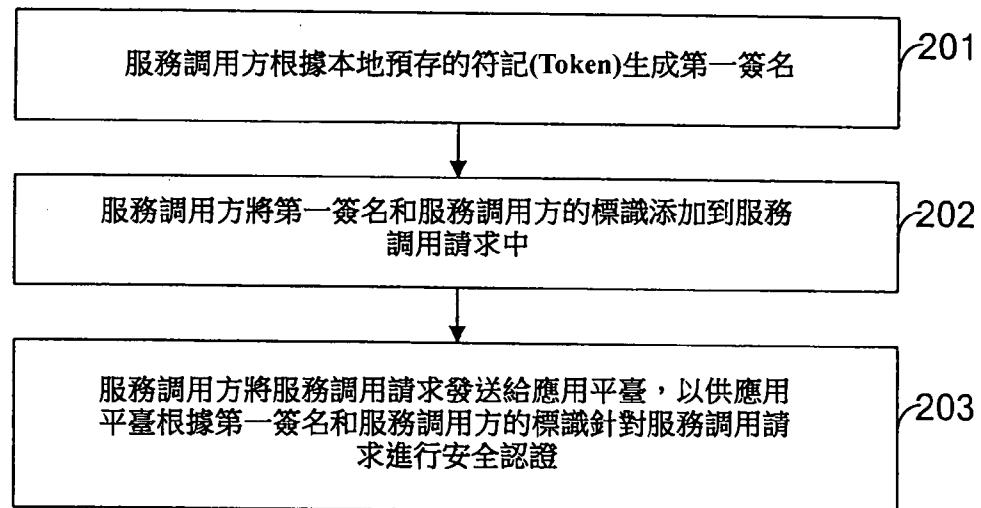


圖 2

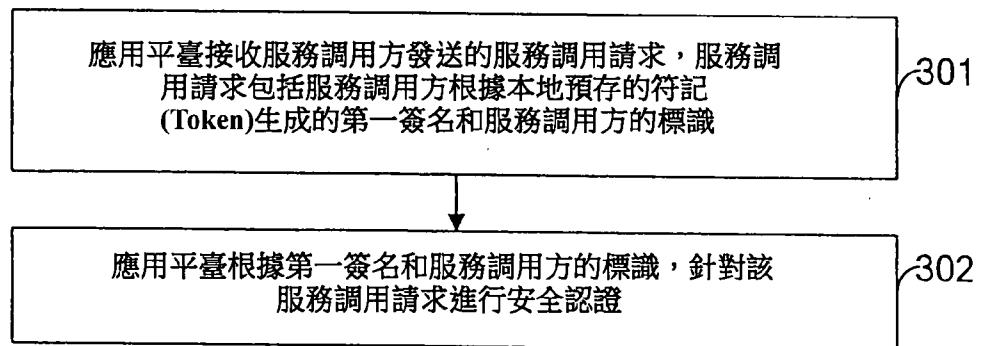


圖 3

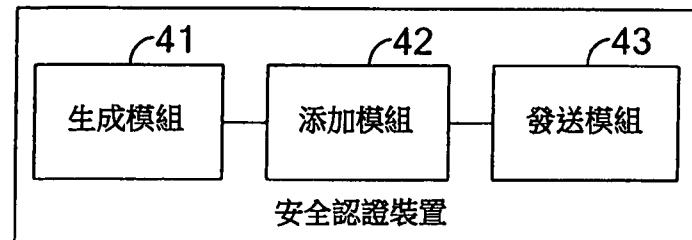


圖 4

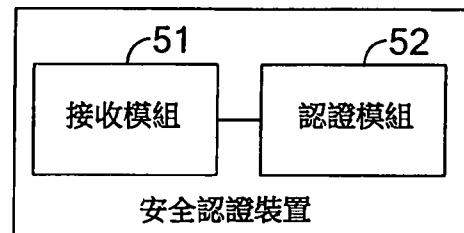


圖 5

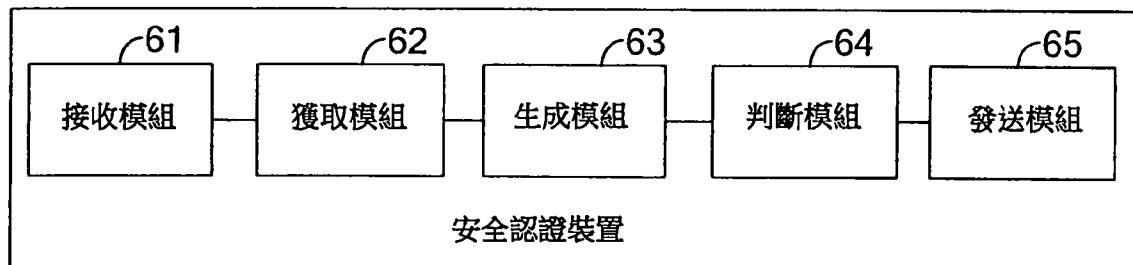


圖 6

第 105107218 號

民國 108 年 6 月 25 日修正

申請專利範圍

1. 一種安全認證方法，其中，包括：

服務調用方根據本地預存的符記生成第一簽名；

該服務調用方將該第一簽名和該服務調用方的標識添加到服務調用請求中；以及

該服務調用方將該服務調用請求發送給應用平臺，以供該應用平臺根據該第一簽名和該服務調用方的標識針對該服務調用請求進行安全認證，

其中，該服務調用方根據本地預存的符記生成第一簽名，包括：

該服務調用方根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成該第一簽名，包括：

該服務調用方將該服務參數和該時間戳記組合為調用參數，按照該調用參數中的分隔符號對該調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

該服務調用方在該第一參數序列前端和後端分別添加該符記，以獲得第二參數序列；以及

該服務調用方對該第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得該第一簽名。

2. 如申請專利範圍第 1 項所述的方法，其中，

該服務調用方將該第一簽名和該服務調用方的標識添加到服務調用請求中，包括：

第 105107218 號

民國 108 年 6 月 25 日修正

該服務調用方將該第一簽名、該服務調用方的標識、該服務參數和該時間戳記添加到該服務調用請求中。

3. 如申請專利範圍第 1 項所述的方法，其中，該服務調用方根據本地預存的符記生成第一簽名之前，包括：

該服務調用方向符記管理系統申請符記，並將申請到的該符記儲存在本地。

4. 一種安全認證方法，其中，包括：

應用平臺接收服務調用方發送的服務調用請求，該服務調用請求包括該服務調用方根據本地預存的符記生成的第一簽名和該服務調用方的標識；

該應用平臺根據該第一簽名和該服務調用方的標識，針對該服務調用請求進行安全認證，包括：

該應用平臺將該服務調用請求發送給符記管理系統，以供該符記管理系統根據該第一簽名和該服務調用方的標識針對該服務調用請求進行安全認證；以及

該應用平臺接收該符記管理系統返回的認證結果資訊；

該方法還包括：

該符記管理系統根據該服務調用方的標識，獲取該服務調用方的符記；

該符記管理系統根據該服務調用方的符記、該服務參數和該時間戳記生成第二簽名；

該符記管理系統判斷該第一簽名與該第二簽名是否相同，並判斷該時間戳記是否在有效期內；

第 105107218 號

民國 108 年 6 月 25 日修正

若該第一簽名和該第二簽名相同，且該時間戳記在有效期內，該符記管理系統向該應用平臺返回指示安全認證通過的認證結果資訊；

若該第一簽名和該第二簽名不相同，或者該時間戳記未在有效期內，該符記管理系統向該應用平臺返回指示安全認證未通過的認證結果資訊，

其中，該符記管理系統根據該服務調用方的符記、該服務參數和該時間戳記生成第二簽名，包括：

該符記管理系統將該服務參數和該時間戳記組合為調用參數，按照該調用參數中的分隔符號對該調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

該符記管理系統在該第一參數序列前端和後端分別添加該符記，以獲得第二參數序列；以及

該符記管理系統對該第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得該第二簽名。

5. 如申請專利範圍第 4 項所述的方法，其中，該第一簽名是該服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的；該服務調用請求還包括：該服務參數和該時間戳記。

6. 如申請專利範圍第 4 項所述的方法，其中，還包括：

該符記管理系統接收該服務調用方發送的符記申請請求；

第 105107218 號

民國 108 年 6 月 25 日修正

該符記管理系統為該服務調用方生成該符記；

該符記管理系統將該符記發送給該服務調用方。

7. 一種安全認證裝置，於服務調用方實現，其中，該裝置包括：

生成模組，用於根據本地預存的符記生成第一簽名；

添加模組，用於將該第一簽名和該服務調用方的標識添加到服務調用請求中；

發送模組，用於將該服務調用請求發送給應用平臺，以供該應用平臺根據該第一簽名和該服務調用方的標識針對該服務調用請求進行安全認證，

其中，該生成模組具體用於：

根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成該第一簽名，包括：

該生成模組將該服務參數和該時間戳記組合為調用參數，按照該調用參數中的分隔符號對該調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

該生成模組在該第一參數序列前端和後端分別添加該符記，以獲得第二參數序列；以及

該生成模組對該第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得該第一簽名。

8. 如申請專利範圍第 7 項所述的裝置，其中，該添加模組具體用於：

將該第一簽名、該服務調用方的標識、該服務參數和

第 105107218 號

民國 108 年 6 月 25 日修正

該時間戳記添加到該服務調用請求中。

9. 如申請專利範圍第 7 項所述的裝置，其中，還包括：

申請模組，用於向符記管理系統申請該符記；

儲存模組，用於在本地儲存該申請模組申請到的該符記。

10. 一種安全認證裝置，於符記管理系統中實現，其中，該裝置包括：

接收模組，用於接收應用平臺發送的服務調用請求，該服務調用請求包括服務調用方根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成的第一簽名、該服務調用方的標識、該服務參數和該時間戳記；

獲取模組，用於根據該服務調用方的標識，獲取該服務調用方的符記；

生成模組，用於根據該服務調用方的符記、該服務參數和該時間戳記生成第二簽名，包括：

該生成模組將該服務參數和該時間戳記組合為調用參數，按照該調用參數中的分隔符號對該調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

該生成模組在該第一參數序列前端和後端分別添加該符記，以獲得第二參數序列；以及

該符記管理系統對該第二參數序列進行編碼，並

第 105107218 號

民國 108 年 6 月 25 日修正

將編碼結果轉換為小寫字元，以獲得該第二簽名；

判斷模組，用於判斷該第一簽名與該第二簽名是否相同，並判斷該時間戳記是否在有效期內；

發送模組，用於在該第一簽名和該第二簽名相同，且該時間戳記在有效期內時，向該應用平臺返回指示安全認證通過的認證結果資訊，或者在該第一簽名和該第二簽名不相同，或者該時間戳記未在有效期內時，向該應用平臺返回指示安全認證未通過的認證結果資訊。

11. 一種安全認證系統，其中，包括：服務調用方和應用平臺；

該服務調用方，用於根據本地預存的符記生成第一簽名，將該第一簽名和該服務調用方的標識添加到服務調用請求中，將該服務調用請求發送給該應用平臺；

該應用平臺，用於接收該服務調用請求，根據該第一簽名和該服務調用方的標識，針對該服務調用請求進行安全認證，

其中，該服務調用方具體用於：根據本地預存的符記、本次服務調用所需的服務參數和本次服務調用的時間戳記生成該第一簽名，將該第一簽名、該服務調用方的標識、該服務參數和該時間戳記添加到該服務調用請求中，

其中，該根據本地預存的符記、本次服務調用所需的服務參數、本次服務調用的時間戳記生成該第一簽名，包括：

該服務調用方將該服務參數和該時間戳記組合為

第 105107218 號

民國 108 年 6 月 25 日修正

調用參數，按照該調用參數中的分隔符號對該調用參數進行切分，以獲得多個參數段，並按照字元順序對每個參數段進行排序，以獲得第一參數序列；

該服務調用方在該第一參數序列前端和後端分別添加該符記，以獲得第二參數序列；以及

該服務調用方對該第二參數序列進行編碼，並將編碼結果轉換為小寫字元，以獲得該第一簽名。

12. 如申請專利範圍第 11 項所述的系統，其中，還包括：符記管理系統；

該應用平臺具體用於：將該服務調用請求發送給該符記管理系統，接收該符記管理系統返回的認證結果資訊；

該符記管理系統，用於根據該服務調用方的標識，獲取該服務調用方的符記，根據該服務調用方的符記、該服務參數和該時間戳記生成第二簽名，判斷該第一簽名與該第二簽名是否相同，並判斷該時間戳記是否在有效期內；若該第一簽名和該第二簽名相同，且該時間戳記在有效期內，向該應用平臺返回指示安全認證通過的認證結果資訊；若該第一簽名和該第二簽名不相同，或者該時間戳記未在有效期內，向該應用平臺返回指示安全認證未通過的認證結果資訊。