201828162

(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 201828162 A

(43)公開日： 中華民國 107 (2018) 年 08 月 01 日

(21)申請案號：106138081 (22)申請日： 中華民國 106 (2017) 年 11 月 03 日

(51)Int. Cl.： *G06Q10/00 (2012.01)* *G06F21/35 (2013.01)*

(30)優先權：2017/01/19 中國大陸 201710039829.6

(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：朱碧軍 (CN)；賈海軍 (CN)；孫健康 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：22 項 圖式數：14 共 53 頁

(54)名稱

設備配置方法及裝置、系統

(57)摘要

本發明提供一種設備配置方法及裝置、系統，該系統包括預設管理使用者的使用者設備、伺服器和智慧設備；其中：所述使用者設備向所述伺服器發送針對所述智慧設備的綁定請求，所述綁定請求用於指示所述伺服器對所述智慧設備進行綁定處理；所述伺服器在執行所述綁定處理的過程中，記錄所述管理使用者對所述智慧設備的管理許可權；所述智慧設備在接收到來自任一使用者的近場通訊信號時，識別所述任一使用者的使用者身份；當確定所述任一使用者為所述管理使用者時，與所述任一使用者的電子設備建立近場通訊連接，以供所述任一使用者對所述智慧設備進行配置。透過本發明的技術方案，可以基於軟體方式對設備進行配置，在簡化配置操作的同時，消除了實體按鍵存在的安全性隱患。

指定代表圖：

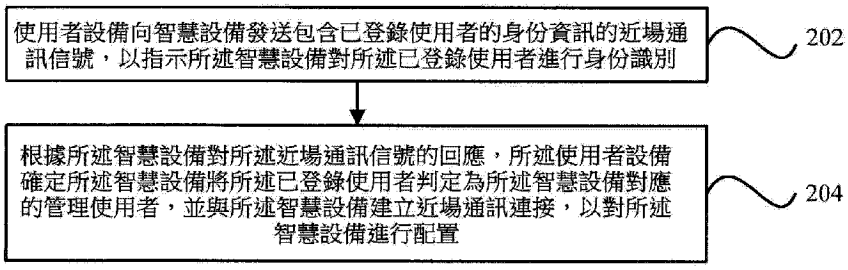

圖 2

【發明說明書】

【中文發明名稱】

設備配置方法及裝置、系統

【技術領域】

本發明涉及智慧設備技術領域，尤其涉及一種設備配置方法及裝置、系統。

【先前技術】

在相關技術中，對於智慧設備的應用越來越多，以企業場景為例，智慧門禁、智慧考勤機、智慧會議終端等，正在被廣泛應用並提升企業內部的工作效率。以智慧考勤機為例，由於涉及到企業內部的企業成員考勤資料，並且需要根據該考勤資料進行財務管理、人員管控等，因而只有企業內部的管理使用者才對智慧考勤機具有管理許可權，可以對智慧考勤機使用的無線網路、綁定的企業或部門、考勤規則等進行設置。

但是，由於相關技術中的智慧考勤機上設置有諸如“重置（RESET）”等實體按鍵，導致無論任何人員觸發該實體按鍵後，均會使得智慧考勤機發生重置，導致存在極高的安全隱患。

【發明內容】

有鑑於此，本發明提供一種設備配置方法及裝置、系

統，可以基於軟體方式對設備進行配置，在簡化配置操作的同時，消除了實體按鍵存在的安全性隱患。

為實現上述目的，本發明提供技術方案如下：

根據本發明的第一方面，提出了一種設備配置系統，包括：預設管理使用者的使用者設備、伺服器和智慧設備；其中：

所述使用者設備向所述伺服器發送針對所述智慧設備的綁定請求，所述綁定請求用於指示所述伺服器對所述智慧設備進行綁定處理；

所述伺服器在執行所述綁定處理的過程中，記錄所述管理使用者對所述智慧設備的管理許可權；

所述智慧設備在接收到來自任一使用者的近場通訊信號時，識別所述任一使用者的使用者身份；當確定所述任一使用者為所述管理使用者時，與所述任一使用者的電子設備建立近場通訊連接，以供所述任一使用者對所述智慧設備進行配置。

根據本發明的第二方面，提出了一種設備配置方法，包括：

使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示所述智慧設備對所述已登錄使用者進行身份識別；

根據所述智慧設備對所述近場通訊信號的回應，所述使用者設備確定所述智慧設備將所述已登錄使用者判定為所述智慧設備對應的管理使用者，並與所述智慧設備建立

近場通訊連接，以對所述智慧設備進行配置。

根據本發明的協力廠商面，提出了一種設備配置方法，包括：

伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取所述智慧設備對應的管理使用者的身份驗證資訊；

所述伺服器向所述預設使用者返回所述身份驗證資訊，以由所述預設使用者向所述智慧設備發送包含所述身份驗證資訊的近場通訊信號，所述近場通訊信號用於指示所述智慧設備根據所述身份驗證資訊確定所述預設使用者具有管理許可權，並與所述近場通訊信號的發送方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。

根據本發明的第四方面，提出了一種設備配置方法，包括：

智慧設備在接收到任一使用者發送的近場通訊信號時，獲取所述近場通訊信號中包含的身份資訊；

所述智慧設備根據所述身份資訊對所述任一使用者進行身份識別；

當判定所述任一使用者為所述智慧設備對應的管理使用者時，所述智慧設備與所述任一使用者使用的電子設備建立近場通訊連接，供所述電子設備對所述智慧設備進行配置。

根據本發明的第五方面，提出了一種設備配置裝置，

包括：

發送單元，使使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示所述智慧設備對所述已登錄使用者進行身份識別；

識別單元，根據所述智慧設備對所述近場通訊信號的回應，使所述使用者設備確定所述智慧設備將所述已登錄使用者判定為所述智慧設備對應的管理使用者，並與所述智慧設備建立近場通訊連接，以對所述智慧設備進行配置。

根據本發明的第六方面，提出了一種設備配置裝置，包括：

獲取單元，使伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取所述智慧設備對應的管理使用者的身份驗證資訊；

返回單元，使所述伺服器向所述預設使用者返回所述身份驗證資訊，以由所述預設使用者向所述智慧設備發送包含所述身份驗證資訊的近場通訊信號，所述近場通訊信號用於指示所述智慧設備根據所述身份驗證資訊確定所述預設使用者具有管理許可權，並與所述近場通訊信號的發送方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。

根據本發明的第七方面，提出了一種設備配置裝置，包括：

獲取單元，使智慧設備在接收到任一使用者發送的近

場通訊信號時，獲取所述近場通訊信號中包含的身份資訊；

識別單元，使所述智慧設備根據所述身份資訊對所述任一使用者進行身份識別；

建立單元，當判定所述任一使用者為所述智慧設備對應的管理使用者時，使所述智慧設備與所述任一使用者使用的電子設備建立近場通訊連接，供所述電子設備對所述智慧設備進行配置。

由以上技術方案可見，本發明透過由智慧設備對操控使用者進行身份識別，使得僅具有管理許可權的使用者能夠將使用的電子設備與智慧設備建立近場通訊連接、執行配置操作，而避免了硬體方式下無關人員對相關實體按鍵的觸發存在的安全性隱患，有助於提升配置操作的安全性。

【圖式簡單說明】

圖1是相關技術中的一種設有配置鍵的智慧考勤機的結構示意圖。

圖2是本發明一示例性實施例提供的一種基於使用者側的設備配置方法的流程圖。

圖3是本發明一示例性實施例提供的一種基於伺服器側的設備配置方法的流程圖。

圖4是本發明一示例性實施例提供的一種基於智慧設備側的設備配置方法的流程圖。

圖5是本發明一示例性實施例提供的一種設備配置系統的結構示意圖。

圖6是本發明一示例性實施例提供的一種設備配置方法的流程圖。

圖7是本發明一示例性實施例提供的一種智慧考勤機的結構示意圖。

圖8是本發明一示例性實施例提供的一種對智慧考勤機進行綁定的頁面示意圖。

圖9是本發明一示例性實施例提供的一種基於使用者側的電子設備的結構示意圖。

圖10是本發明一示例性實施例提供的一種基於使用者側的設備配置裝置的方塊圖。

圖11是本發明一示例性實施例提供的一種基於伺服器側的電子設備的結構示意圖。

圖12是本發明一示例性實施例提供的一種基於伺服器側的設備配置裝置的方塊圖。

圖13是本發明一示例性實施例提供的一種基於智慧設備側的電子設備的結構示意圖。

圖14是本發明一示例性實施例提供的一種基於智慧設備側的設備配置裝置的方塊圖。

【實施方式】

在相關技術中，對於智慧設備的應用越來越多，以企業場景為例，智慧門禁、智慧考勤機、智慧會議終端等，

正在被廣泛應用並提升企業內部的工作效率。以智慧考勤機為例，由於涉及到企業內部的企業成員考勤資料，並且需要根據該考勤資料進行財務管理、人員管控等，因而只有企業內部的管理使用者才對智慧考勤機具有管理許可權，可以對智慧考勤機使用的無線網路、綁定的企業或部門、考勤規則等進行設置。

通常而言，管理使用者無論是直接在智慧考勤機上進行編輯，還是在管理使用者使用的電子設備與該智慧考勤機運行有同一預設通訊應用程式的使用者端時，管理使用者透過該電子設備上的使用者端對該智慧考勤機進行編輯，都需要對管理使用者進行身份驗證，並確認具有對該智慧考勤機的管理許可權時，才能夠執行編輯操作。

但是，由於智慧考勤機上設置有如圖1所示的重置(RESET)等實體按鍵（圖1中位於智慧考勤機的側面），使得任何人員均可以透過觸發該RESET按鍵實現對該智慧考勤機的重置操作，並且難以確定該觸發行為是有意觸發或誤觸發，使得智慧考勤機存在很大的安全隱患，無法確保智慧考勤機的正常運行。

因此，本發明透過提出一種新的設備配置方案，可以解決相關技術中的上述技術問題。為對本發明進行進一步說明，提供下列實施例：

圖2是本發明一示例性實施例提供的一種基於使用者側的設備配置方法的流程圖。如圖2所示，該方法應用於使用者設備（即預設使用者使用的電子設備）上，可以包

括以下步驟：

步驟202，使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示所述智慧設備對所述已登錄使用者進行身份識別。

在本實施例中，使用者設備、智慧設備上可以分別運行有移動化團體辦公平臺的使用者端，比如使用者設備上運行有使用者端1、智慧設備上運行有使用者端2；其中，使用者端1上登錄有預設使用者的註冊帳號，使得該使用者設備或該使用者設備上運行的使用者端1被配置為唯一對應於該預設使用者。類似地，智慧設備或該智慧設備上運行的使用者端2同樣具有唯一性，用於唯一確定該智慧設備、區別於其他智慧設備。相應地，伺服器上可以運行有該移動化團體辦公平臺的服務端。那麼，基於該移動化團體辦公平臺的使用者端1、使用者端2、服務端等，可以實現使用者設備、智慧設備、伺服器之間的資料互動。

實際上，移動化企業辦公平臺不僅可以實現通訊功能，還可以作為諸多其他功能的整合化功能平臺，比如對於審批事件（如請假、辦公物品申領、財務等審批事件）、考勤事件、任務事件、日誌事件等企業內部事件的處理，再比如訂餐、採購等企業外部事件的處理，本發明並不對此進行限制。

較為具體地，移動化企業辦公平臺可以承載於相關技術中的即時通訊應用程式，比如企業即時通訊（Enterprise Instant Messaging，EIM）應用程式，例如

Skype For Business®、Microsoft Teams®、Yammer®、Workplace®、Slack®、企業微信®、紛享銷客®、企業飛信®、企業易信®等。當然，即時通訊功能僅為移動化企業辦公平臺支援的通訊功能之一，該企業辦公平臺還能夠實現更多諸如上述的其他功能，此處不再贅述。

在本實施例中，以使用者設備為例：透過在使用者設備上安裝移動化企業辦公平臺的使用者端應用程式（APP），並登錄預設使用者在該移動化企業辦公平臺處的註冊帳號，即可將該使用者設備配置為該預設使用者對應的移動化企業辦公平臺的使用者端1。其中，該使用者設備可以為手機、平板等移動設備，或者該使用者設備也可以為PC主機等非移動式的使用者設備，本發明並不對此進行限制。當然，當採用諸如HTML5技術的線上“使用者端”，無需在使用者設備上安裝相應的應用程式，即可在使用者設備上運行上述的使用者端1。

步驟204，根據所述智慧設備對所述近場通訊信號的回應，所述使用者設備確定所述智慧設備將所述已登錄使用者判定為所述智慧設備對應的管理使用者，並與所述智慧設備建立近場通訊連接，以對所述智慧設備進行配置。

在本實施例中，智慧設備可以應用於任意場景中，本發明並不對此進行限制。舉例而言，在團體（如企業、學校、政府機關、公安部門等）場景下，該智慧設備可以被綁定至預設團體，則上述的配置請求中可以包含本端使用者（即上述的預設使用者）的身份資訊，以指示伺服器在

該身份資訊匹配於該預設團體的管理使用者（即該預設團體中具有管理許可權的使用者）時，返回所述智慧設備對應的身份資訊，而非管理使用者則可以不返回該身份資訊，以實現對配置操作的許可權管理。

在本實施例中，使用者設備可以向伺服器發送針對所述智慧設備的配置請求，所述配置請求用於指示所述伺服器返回所述智慧設備對應的標準數位摘要；然後，所述使用者設備接收所述伺服器返回的所述標準數位摘要，以作為所述已登錄使用者的身份資訊；其中，所述標準數位摘要與所述智慧設備預先產生並上傳的隨機碼相關，且所述隨機碼還被記錄為所述智慧設備上的本地隨機碼。那麼，使用者設備將所述標準數位摘要作為所述身份資訊添加至所述近場通訊信號中，以指示所述智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在所述標準數位摘要與所述本地數位摘要相匹配時，透過回應於所述近場通訊信號，與所述近場通訊信號的發送方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。透過在智慧設備上產生隨機碼，使得相應產生的標準數位摘要唯一對應於該智慧設備，並且由於其隨機特性而具有較高的安全性和防作弊性。

在本實施例中，智慧設備可以在被首次啟動和綁定的過程中，產生隨機碼並上傳至伺服器中；當然，智慧設備也可以在其他任意時刻產生並上傳該隨機碼，本發明並不對此進行限制。透過採用基於隨機碼的標準數位摘要，使

得該標準數位摘要具有“隨機”特性，既能夠唯一對應於該智慧設備，又能夠避免透過“窮舉”等方式進行猜測獲得，有助於進一步提升配置操作的安全性。

在本實施例中，伺服器根據隨機碼產生標準數位摘要時採用的演算法，與智慧設備根據本地隨機碼產生本地數位摘要時採用的演算法一致，使得標準數位摘要對應的隨機碼與該本地隨機碼相同時，即可確保標準數位摘要與該本地數位摘要相同，使得智慧設備能夠準確識別出本端使用者的身份，確保只有管理使用者能夠順利完成對智慧設備的配置操作。

在本實施例中，智慧設備可以預先獲取標準數位摘要並保存在本地，並在後續的任意時刻根據本機存放區的該標準數位摘要對智慧設備進行配置處理；或者，可以限制智慧設備對標準數位摘要的本地使用次數，使得智慧設備根據本機存放區的標準數位摘要向智慧設備發送近場通訊信號的次數達到該本地使用次數時，使用者設備必須刪除本機存放區的標準數位摘要，後續必須重新從伺服器處獲取該標準數位摘要；或者，為了進一步提升安全性，可以限制智慧設備不允許對標準數位摘要進行保存，每次均必須從伺服器處獲取該標準數位摘要。

在本實施例中，當標準數位摘要與本地數位摘要相匹配時，智慧設備可以基於接收到的近場通訊信號，與發送該近場通訊信號的使用者設備之間建立近場通訊連接，以使得預設使用者在該使用者設備上進行操作時，可以基於

該近場通訊連接對該智慧設備進行配置。其中，當近場通訊連接是基於藍牙低功耗（Bluetooth Low Energy，BLE）技術時，比如基於ibeacon協議，那麼上述的近場通訊信號可以為通告幀（Advertising）消息；當然，本發明並不對該近場通訊技術的類型進行限制，比如還可以採用諸如NFC（Near Field Communication，近距離無線通訊技術）等其他類型的近場通訊技術。

相應地，圖3是本發明一示例性實施例提供的一種基於伺服器側的設備配置方法的流程圖。如圖3所示，該方法應用於伺服器上，可以包括以下步驟：

步驟302，伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取所述智慧設備對應的管理使用者的身份驗證資訊。

在本實施例中，預設使用者可以為預設團體的管理使用者，且智慧設備被預先綁定至該預設團體。換言之，當智慧設備被預先綁定至預設團體時，伺服器可以對發送配置請求的該預設使用者進行身份驗證，只有當該預設使用者為該預設團體的管理使用者時，才向該預設使用者返回該智慧設備對應的身份驗證資訊，以確保針對該智慧設備的配置操作的安全性。

在本實施例中，身份驗證資訊可以包括所述智慧設備對應的標準數位摘要，所述標準數位摘要與所述智慧設備預先產生並上傳的隨機碼相關，且所述隨機碼還被記錄為所述智慧設備上的本地隨機碼。透過在智慧設備上產生隨

機碼，使得相應產生的標準數位摘要唯一對應於該智慧設備，並且由於其隨機特性而具有較高的安全性和防作弊性。當然，身份驗證資訊也可以包括其他內容，比如與管理使用者的使用者ID相關的字串等，只要能夠由智慧設備據此進行身份驗證即可，本發明並不對此進行限制。

在一實施例中，標準數位摘要可以為所述隨機碼的數位摘要，即伺服器直接為隨機碼產生相應的數位摘要，以作為該標準數位摘要。相應地，智慧設備在接收到該預設使用者發送的近場通訊信號後，同樣為記錄的本地隨機碼產生相應的數位摘要，以作為相應的本地數位摘要。

在另一實施例中，標準數位摘要可以為下述資訊中至少之一和隨機碼的共同數位摘要：智慧設備的啟動碼、智慧設備的序號、智慧設備的被綁定物件的標識資訊（如該被綁定物件可以為上述的預設團體，則相應的標識資訊可以為該預設團體的組織標識（Organization ID，或簡稱為Org ID）），從而增加了數位摘要本發明的複雜程度，以進一步提升安全性。尤其是，當同時由多種資訊產生數位摘要時，這些資訊之間存在更多種組合的可能性，從而降低了被猜測出的可能性。

步驟304，所述伺服器向所述預設使用者返回所述身份驗證資訊，以由所述預設使用者向所述智慧設備發送包含所述身份驗證資訊的近場通訊信號，所述近場通訊信號用於指示所述智慧設備根據所述身份驗證資訊確定所述預設使用者具有管理許可權，並與所述近場通訊信號的發送

方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。

在本實施例中，當身份驗證資訊包括智慧設備對應的標準數位摘要時，所述近場通訊信號用於指示所述智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在所述標準數位摘要與所述本地數位摘要相匹配時，確定所述預設使用者具有管理許可權。

在本實施例中，伺服器還可以根據智慧設備產生並上傳的更新隨機碼，對記錄的標準數位摘要進行更新，且該更新隨機碼還被智慧設備用於對本地隨機碼進行更新，從而透過對標準數位摘要、本地隨機碼進行更新，可以避免標準數位摘要或隨機碼洩露而造成安全隱患，有助於提升安全性。

相應地，圖4是本發明一示例性實施例提供的一種基於智慧設備側的設備配置方法的流程圖。如圖4所示，該方法應用於伺服器上，可以包括以下步驟：

步驟402，智慧設備在接收到任一使用者發送的近場通訊信號時，獲取所述近場通訊信號中包含的身份資訊。

步驟404，所述智慧設備根據所述身份資訊對所述任一使用者進行身份識別。

步驟406，當判定所述任一使用者為所述智慧設備對應的管理使用者時，所述智慧設備與所述任一使用者使用的電子設備建立近場通訊連接，供所述電子設備對所述智慧設備進行配置。

在本實施例中，所述智慧設備可以預先將產生的隨機碼上傳至伺服器，以使所述伺服器產生與所述隨機碼相關的標準數位摘要，並將所述標準數位摘要發送至對所述智慧設備具有管理許可權的預設管理使用者，以作為所述預設管理使用者的身份資訊；其中，所述隨機碼還被記錄為所述智慧設備的本地隨機碼。

相應地，智慧設備對該任一使用者進行身份識別時，可以產生與記錄的本地隨機碼相關的本地數位摘要，並將所述本地數位摘要與所述近場通訊信號中作為所述身份資訊的待驗證數位摘要進行比較；其中，當所述待驗證數位摘要與所述本地數位摘要相匹配時，所述智慧設備判定所述任一使用者為所述智慧設備對應的管理使用者。

在本實施例中，當待驗證數位摘要與本地數位摘要相同時，表明該待驗證數位摘要即為伺服器處針對該智慧設備產生的標準數位摘要，則確定該任一使用者為管理使用者，即具有對該智慧設備的管理許可權，透過切換至配置模式使得該管理使用者對該智慧設備進行配置操作；當待驗證數位摘要與本地數位摘要不同時，表明該任一使用者不具有管理許可權，不允許該任一使用者對該智慧設備進行配置操作。

在本實施例中，智慧設備可以在首次啟動並被綁定的過程中，產生啟動碼並上傳至伺服器，則後續均可以使用該啟動碼和相應的標準數位摘要，以實現對該智慧設備的配置操作。而為了提升安全性，避免啟動碼或標準數位摘

要洩露或被竊取，智慧設備可以產生更新隨機碼並上傳至所述伺服器，以使所述伺服器對所述標準數位摘要進行更新，且該更新隨機碼還被用於對所述本地隨機碼進行更新，以使得先前洩露或被竊取的啟動碼、標準數位摘要等均失效。

在一實施例中，智慧設備可以按照預定義週期產生所述更新隨機碼並上傳至所述伺服器，比如每天、每週、每月或按照其他週期進行更新。

在另一實施例中，智慧設備可以在每次完成配置操作後，均產生更新隨機碼並上傳至所述伺服器；較為具體地，智慧設備可以在斷開與使用者設備的近場通訊連接時，確定本次配置操作已完成，並產生和上傳更新隨機碼，當然本發明並不對此進行限制。那麼，即便使用者設備從伺服器處獲得標準數位摘要時，該標準數位摘要可能被其他人竊取，只要該使用者設備對智慧設備完成配置後，該智慧設備產生更新啟動碼並上傳至伺服器，那麼已被竊取的標準數位摘要就會失效，而不會被應用於對該智慧設備的配置操作。

由以上技術方案可見，本發明透過由智慧設備對操控使用者進行身份識別，使得僅具有管理許可權的使用者能夠將使用的電子設備與智慧設備建立近場通訊連接、執行配置操作，而避免了硬體方式下無關人員對相關實體按鍵的觸發存在的安全性隱患，有助於提升配置操作的安全性。

下面以企業場景為例，假定企業AA中存在企業管理成員A，該企業管理成員A透過手機對綁定至該企業AA的智慧考勤機進行配置操作，對本發明的技術方案進行詳細說明。其中，圖5是本發明一示例性實施例提供的一種設備配置系統的結構示意圖，如圖5所示，假定該系統由企業微信或其他類似的移動化團體辦公平臺支援，該系統包括企業管理成員A使用的手機、智慧考勤機和企業微信伺服器，手機和智慧考勤機上分別運行有企業微信使用者端、企業微信伺服器上運行有企業微信服務端，其中智慧考勤機上不需要裝配RESET實體按鍵，而由企業即時通訊應用程式“企業微信”提供相應的“軟開關”或“軟體開關”，從而透過軟體方式實現配置功能。

企業微信伺服器可以為包含一獨立主機的實體伺服器，或者該企業微信伺服器可以為主機集群承載的虛擬伺服器，或者該企業微信伺服器可以為雲伺服器。在運行過程中，企業微信伺服器可以運行某一應用程式的伺服器側的程式，以實現該應用程式的相關業務功能，比如當該企業微信伺服器運行移動化團體辦公平臺的程式時，可以實現為該移動化團體辦公平臺的服務端。而在本發明的技術方案中，由企業微信伺服器運行團體資訊平臺，並對該團體資訊平臺上的團體資訊進行集中管理，包括對來自各個團體的團體資訊進行記錄和維護，以及在多個團體之間實現團體資訊的互動處理。

手機只是使用者可以使用的一種類型的電子設備。實

際上，使用者顯然還可以使用諸如下述類型的電子設備：平板設備、筆記型電腦、掌上型電腦（PDAs，Personal Digital Assistants）、可穿戴設備（如智慧眼鏡、智慧手錶等）等，本發明並不對此進行限制。在運行過程中，該電子設備可以運行某一應用程式的使用者端側的程式，以實現該應用程式的相關業務功能，比如上述的設備配置功能等。類似地，智慧考勤機也可以運行某一應用程式的使用者端側的程式，以實現該應用程式的相關業務功能，比如上述的設備配置功能等。

而對於手機、智慧考勤機與企業微信伺服器之間進行互動的網路，可以包括多種類型的有線或無線網路。在一實施例中，該網路可以包括公共交換電話網路（Public Switched Telephone Network，PSTN）和網際網路。

具體的，如圖5所示的系統可以透過圖6所示的設備配置方法實現對智慧考勤機的配置，該方法可以包括以下步驟：

步驟602，手機獲取智慧考勤機的啟動碼（active code）、序號（serial number）等信息。

在本實施例中，當描述為“手機獲取”時，實際上是指手機上運行的企業微信使用者端執行“獲取”操作，當然該過程需要手機本身的硬體支援；在本發明中的其他部分，情況與此處相似。

在本實施例中，智慧考勤機首先透過下述方式確定自身對應的啟動碼、序號等資訊；以啟動碼為例（序號的情

況類似）：

在一種情況下，智慧考勤機在首次開機後，可以檢查儲存空間中是否存在啟動碼；如果不存在，該智慧考勤機向企業微信伺服器發送啟動碼獲取請求，以使企業微信伺服器向該智慧考勤機分配唯一對應的啟動碼，且企業微信伺服器會將該啟動碼與該智慧考勤機之間建立唯一映射關係。

在另一種情況下，智慧考勤機在出廠時，已經在儲存空間內儲存有自身的啟動碼，且企業微信伺服器上也已經預先記錄有上述的唯一映射關係，因而無需智慧考勤機向企業微信伺服器獲取該啟動碼。

其中，智慧考勤機可以一直應用同一啟動碼；或者，智慧考勤機可以按照預設週期主動老化儲存空間內的啟動碼，並向企業微信服務器重新請求新的啟動碼，那麼企業微信伺服器可以使用該新的啟動碼來替換舊的啟動碼（即被老化的啟動碼），並更新上述的唯一映射關係。

在一實施例中，啟動碼、序號等資訊可以表現為圖7所示的二維碼或其他形式的圖形碼，那麼該智慧考勤機可以直接顯示出該圖形碼。或者，啟動碼、序號等資訊可以為字串或其他形式的非圖形資訊，那麼該智慧考勤機可以直接顯示出該字串，也可以對該字串進行轉換，並顯示出轉換得到的諸如圖7所示的圖形碼等。當然，啟動碼還可以採用其他形式，而該智慧考勤機也可以透過更多方式對該啟動碼進行顯示，本發明並不對此進行限制。那麼，手

機可以透過下述方式獲取智慧考勤機的啟動碼、序號等資訊：

在一種情況下，當該智慧考勤機上的啟動碼為圖形碼形式時，可以透過手機上運行的企業微信使用者端上的“掃碼”功能，啟動手機上的攝像頭元件對該圖形碼進行採集，然後透過內容識別而讀取啟動碼的內容；以啟動碼為例，透過對圖7所示的二維碼進行讀取後，可以識別出該二維碼對應的啟動碼為“gfd1s5g451f24sg54sg241fd1”。

在另一種情況下，當該智慧考勤機上的啟動碼為字串形式時，可以透過手機上運行的企業微信使用者端的相關功能，啟動手機上的攝像頭元件對該字串進行採集，然後透過諸如OCR（Optical Character Recognition，光學字元辨識）等方式識別該字串。當然，手機上運行的企業微信使用者端也可以示出輸入方塊，使得企業管理成員A可以將該智慧考勤機上示出的字串手動輸入至手機中，幫助手機完成對該字串的讀取操作。

在另一實施例中，可以透過在手機與智慧考勤機之間建立近場通訊連接，而手機透過該近場通訊連接從智慧考勤機中獲取啟動碼、序號等資訊。具體地，智慧考勤機可以持續發射通告幀消息，例如該通告幀消息可以基於BLE技術的ibeacon協議進行發送，而手機透過掃描並回應於該通告幀消息，從而在手機與智慧考勤機之間建立藍牙連接；然後，企業管理成員A可以透過在手機上輸入對該智慧考勤機的登錄資訊（如登錄帳號和密碼，通常記錄在智

慧考勤機的外殼或說明書中），使得該智能考勤機確定手機（即企業管理成員A）具有相關許可權後，將啟動碼、序號等資訊返回至該手機。

步驟604，手機向企業微信伺服器發送針對該智慧考勤機的綁定請求，該綁定請求中包含該智慧考勤機的啟動碼、序號等資訊，以及希望與該智慧考勤機進行綁定的企業AA的組織ID。

步驟606，企業微信伺服器根據上述的綁定請求，在智慧考勤機與企業AA之間建立綁定關係。

在一實施例中，手機可以示出如圖8所示的團體選擇頁面，該團體選擇頁面中包含所有與企業管理成員A相關聯的團體，然後手機可以根據接收到的使用者選擇指令，確定該團體選擇頁面中被選中的一個或多個團體，並在上述的綁定請求中添加被選中的團體的組織ID。

在另一實施例中，手機上的企業微信使用者端可以確定與企業管理成員A相關聯的團體的數量；當僅存在一個相關聯的團體時，該企業微信使用者端可以直接將該團體的組織ID添加至上述的綁定請求中，而無需示出如圖8所示的團體選取頁面；而當存在多個相關聯的團體時，該企業微信使用者端可以示出如圖8所示的團體選取頁面，並根據使用者選取指令進行處理，此處不再贅述。

步驟608，手機在接收到企業微信伺服器返回的綁定成功的綁定結果時，向智慧考勤機發送啟動指令。

在本實施例中，企業微信伺服器在將智慧考勤機與企

業AA之間建立綁定關係後，只有企業管理成員A等對該企業AA具有管理許可權的企業成員，才能夠執行針對該智慧考勤機的控制操作，比如對該智慧考勤機的配置操作。

步驟610，智慧考勤機針對接收到的啟動指令，產生隨機碼。

在本實施例中，智慧考勤機可以按照內置的預定義演算法，產生符合預設規則的隨機碼；由於是隨機碼，使得該隨機碼具有唯一性和隨機性，因而難以被模仿和猜測，具有極高的資訊安全性。

步驟612，智慧考勤機一方面將隨機碼記錄為本地隨機碼，另一方面將隨機碼發送至企業微信伺服器。

在本實施例中，企業微信伺服器在接收到上述的綁定請求，並將智慧考勤機與企業AA進行綁定後，並不會終止本次綁定流程，而是繼續等待接收智慧考勤機上傳的隨機碼。

步驟614，企業微信伺服器產生與隨機碼相關的標準數位摘要，並將其與企業AA、智慧考勤機進行關聯記錄。

在本實施例中，智慧考勤機透過將隨機碼記錄為本地隨機碼，使得該本地隨機碼與該智慧考勤機之間建立起唯一對應關係；同時，企業微信伺服器透過將隨機碼對應的標準數位摘要與企業AA、智慧考勤機進行關聯記錄，使得該標準數位摘要、企業AA和智慧考勤機之間建立起唯一對應關係。那麼，透過標準數位摘要與本地隨機碼之間

的匹配關係，以及企業管理成員A對該企業AA的管理許可權，即可確定企業管理成員A與該智慧考勤機之間的唯一對應關係，從而使得該企業管理成員A能夠對該智慧考勤機進行配置操作。

步驟616，企業微信伺服器在完成對標準數位摘要的記錄後，向智慧考勤機返回啟動確認。

在本實施例中，在接收到啟動確認後，智慧考勤機可以斷開與企業微信伺服器之間的通訊連接，企業微信伺服器完成對該智慧考勤機的綁定處理。實際上，智慧考勤機在正常的考勤處理過程中，可以完全在本地完成、不需要與企業微信伺服器進行聯網通訊，那麼即便智慧考勤機在完成綁定後被安裝於網路環境較差的區域，仍然不會影響智慧考勤機的考勤功能。

步驟618，企業管理成員A透過手機向企業微信伺服器發起針對智慧考勤機配置請求，而企業微信伺服器基於該配置請求返回該智慧考勤機對應的標準數位摘要。

在本實施例中，由於企業管理成員A對企業AA具有管理許可權，因而企業管理成員A能夠從企業微信伺服器處請求獲得該智慧考勤機對應的標準數位摘要；而對於其他沒有管理許可權的企業成員，則無法獲得該標準數位摘要，從而避免無關人員對該智慧考勤機進行配置，避免了相關技術中採用實體按鍵而導致的安全性隱患和風險。

步驟620，手機向周圍發射通告幀消息，該通告幀消息中包含上述的標準數位摘要。

在本實施例中，手機從企業微信伺服器處獲取上述的標準數位摘要後，可以將該標準數位摘要儲存於手機上的緩存空間中，即便手機處於網路環境較差的狀態下、無法與企業微信伺服器建立有效的通訊連接，企業管理成員A仍然能夠隨時透過該手機對智慧考勤機進行配置操作，從而極大地提升了對智慧考勤機進行配置的便捷性。

步驟622，智慧考勤機在接收到來自手機的通告幀消息時，根據預先儲存的本地隨機碼，產生與該本地隨機碼相關的本地數位摘要。

步驟624，當通告幀消息中包含的數位摘要與本地數位摘要相匹配時，智慧考勤機與手機之間建立藍牙連接，使得企業管理成員A透過手機對智慧考勤機進行配置操作。

在本實施例中，同一隨機碼被分別上傳至企業微信伺服器和記錄於智慧考勤機本地，由於該隨機碼具有唯一性、唯一對應於該智慧考勤機，使得一方面企業微信伺服器產生與該隨機碼相關的標準數位摘要時，另一方面智慧考勤機應當採用同樣的演算法對本地隨機碼進行處理而得到本地數位摘要，那麼由於採用的隨機碼相同、演算法相同，相應的標準數位摘要與本地數位摘要也相同。同時，當智慧考勤機被綁定至企業AA時，由於只有該企業AA的企業管理成員A（當然，在其他實施例中，企業AA中也可能存在多個具有管理許可權的企業管理成員）具有相關管理許可權，能夠透過上述的步驟618從企業微信伺服器處

獲取標準數位摘要，那麼當通告幀消息中包含的數位摘要與本地數位摘要相匹配時，即可確定該通告幀消息的發送方為該企業管理成員A，因而允許該通告幀消息的發送方設備與該智慧考勤機之間建立藍牙連接，以實現對該智慧考勤機的配置操作。

其中，企業微信伺服器和智慧考勤機可以分別採用MD5(MD即Message Digest)演算法，或者其他任意數位摘要演算法，本發明並不對此進行限制，只要確保企業微信伺服器與智慧考勤機採用的演算法相同即可。而在計算過程中，以企業微信伺服器為為例：一種情況下，可以直接計算隨機碼對應的數位摘要，以作為上述的標準數位摘要；另一種情況下，可以將隨機碼和下述資訊中至少之一進行組合，以計算該組合資訊對應的數位摘要：智慧考勤機的啟動碼、智慧考勤機的序號、企業AA的組織ID等。

在本實施例中，透過智慧考勤機對通告幀消息中包含的數位摘要與本地數位摘要進行匹配，並由此確定通告幀消息對應的發送方是否具有管理許可權，使得整個過程不需要企業微信伺服器的參與，那麼智慧考勤機不存在對網路環境的要求，便於企業管理使用者A僅透過近場通訊環境下，即可實現對智慧考勤機的配置操作，避免網路環境較差而帶來的延遲高、資料易丟包、安全性降低等問題。

同時，由於在近場通訊條件下，通告幀消息的發送方設備必須位於該智慧考勤機附近，而尤其是在團體場景中，智慧考勤機等智慧設備往往安裝在團體的內部工作區

域，因而能夠排除絕大部分非團體成員對該智慧設備進行配置的安全性風險。

進一步地，而為了提升安全性，避免啟動碼或標準數位摘要洩露或被竊取，或者儲存有標準數位摘要的手機發生丟失、失竊等情況下，智慧考勤機可以產生更新隨機碼並上傳至企業微信伺服器，以使企業微信伺服器對預先記錄的標準數位摘要進行更新，且該更新隨機碼還被用於對智慧考勤機上記錄的本地隨機碼進行更新，以使得先前洩露或被竊取的啟動碼、標準數位摘要等均失效。

在一種情況下，智慧考勤機可以按照預定義週期產生更新隨機碼並上傳至企業微信伺服器，比如每天、每週、每月或按照其他週期進行更新。而在另一種情況下，智慧考勤機可以在每次完成配置操作後，均產生更新隨機碼並上傳至企業微信伺服器；較為具體地，智慧考勤機可以在步驟624之後斷開與手機的藍牙連接時，確定本次配置操作已完成，並產生和上傳更新隨機碼，當然本發明並不對此進行限制；那麼，即便標準數位摘要可能被其他人竊取，只要智慧考勤機產生更新啟動碼並上傳至企業微信伺服器，那麼已被竊取的標準數位摘要就會失效，而無法被應用於對該智慧考勤機的配置操作。

綜上所述，本發明無需在智慧設備上安裝實體按鍵，而可以完全透過電子設備與該智慧設備之間的近場通訊方式，實現對智慧設備的配置操作，從而避免實體按鍵帶來的安全隱患和風險，並提升對智慧設備的配置操作的便捷

性。

圖9示出了根據本發明的一示例性實施例的電子設備的示意結構圖。請參考圖9，在硬體層面，該電子設備包括處理器902、內部匯流排904、網路介面906、記憶體908以及非易失性記憶體910，當然還可能包括其他業務所需要的硬體。處理器902從非易失性記憶體910中讀取對應的電腦程式到記憶體902中然後運行，在邏輯層面上形成設備配置裝置。當然，除了軟體實現方式之外，本發明並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

請參考圖10，在軟體實施方式中，該設備配置裝置可以包括發送單元1001和識別單元1002。其中：

發送單元1001，使使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示所述智慧設備對所述已登錄使用者進行身份識別；

識別單元1002，根據所述智慧設備對所述近場通訊信號的回應，使所述使用者設備確定所述智慧設備將所述已登錄使用者判定為所述智慧設備對應的管理使用者，並與所述智慧設備建立近場通訊連接，以對所述智慧設備進行配置。

可選的，還包括：

請求單元1003，使所述使用者設備向伺服器發送針對所述智慧設備的配置請求，所述配置請求用於指示所述伺

服器返回所述智慧設備對應的標準數位摘要；

接收單元1004，使所述使用者設備接收所述伺服器返回的所述標準數位摘要，以作為所述已登錄使用者的身份資訊；其中，所述標準數位摘要與所述智慧設備預先產生並上傳的隨機碼相關，且所述隨機碼還被記錄為所述智慧設備上的本地隨機碼；

添加單元1005，使所述使用者設備將所述標準數位摘要作為所述身份資訊添加至所述近場通訊信號中，以指示所述智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在所述標準數位摘要與所述本地數位摘要相匹配時，透過回應於所述近場通訊信號，與所述近場通訊信號的發送方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。

可選的，所述智慧設備被綁定至預設團體；所述配置請求中包含本端使用者的身份資訊，以指示所述伺服器在所述身份資訊匹配於所述預設團體的管理使用者時，返回所述智慧設備對應的標準數位摘要。

圖11示出了根據本發明的一示例性實施例的電子設備的示意結構圖。請參考圖11，在硬體層面，該電子設備包括處理器1102、內部匯流排1104、網路介面1106、記憶體1108以及非易失性記憶體1110，當然還可能包括其他業務所需要的硬體。處理器1102從非易失性記憶體1110中讀取對應的電腦程式到記憶體1102中然後運行，在邏輯層面上形成設備配置裝置。當然，除了軟體實現方式之外，本發

明並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

請參考圖12，在軟體實施方式中，該設備配置裝置可以包括獲取單元1201和返回單元1202。其中：

獲取單元1201，使伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取所述智慧設備對應的管理使用者的身份驗證資訊；

返回單元1202，使所述伺服器向所述預設使用者返回所述身份驗證資訊，以由所述預設使用者向所述智慧設備發送包含所述身份驗證資訊的近場通訊信號，所述近場通訊信號用於指示所述智慧設備根據所述身份驗證資訊確定所述預設使用者具有管理許可權，並與所述近場通訊信號的發送方設備建立近場通訊連接，供所述發送方設備對所述智慧設備進行配置。

可選的，

所述身份驗證資訊包括所述智慧設備對應的標準數位摘要，所述標準數位摘要與所述智慧設備預先產生並上傳的隨機碼相關，且所述隨機碼還被記錄為所述智慧設備上的本地隨機碼；

其中，所述近場通訊信號用於指示所述智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在所述標準數位摘要與所述本地數位摘要相匹配時，確定所述預設使用者具有管理許可權。

可選的，所述預設使用者為預設團體的管理使用者，且所述智慧設備被預先綁定至所述預設團體。

可選的，其特徵在於：

所述標準數位摘要為所述隨機碼的數位摘要；

或者，所述標準數位摘要為下述資訊中至少之一和所述隨機碼的共同數位摘要：所述智慧設備的啟動碼、所述智慧設備的序號、所述智慧設備的被綁定物件的標識資訊。

可選的，還包括：

更新單元1203，根據所述智慧設備產生並上傳的更新隨機碼，使所述伺服器對記錄的所述標準數位摘要進行更新；其中，所述更新隨機碼還被所述智慧設備用於對所述本地隨機碼進行更新。

圖13示出了根據本發明的一示例性實施例的電子設備的示意結構圖。請參考圖13，在硬體層面，該電子設備包括處理器1302、內部匯流排1304、網路介面1306、記憶體1308以及非易失性記憶體1310，當然還可能包括其他業務所需要的硬體。處理器1302從非易失性記憶體1310中讀取對應的電腦程式到記憶體1302中然後運行，在邏輯層面上形成設備配置裝置。當然，除了軟體實現方式之外，本發明並不排除其他實現方式，比如邏輯器件抑或軟硬體結合的方式等等，也就是說以下處理流程的執行主體並不限定於各個邏輯單元，也可以是硬體或邏輯器件。

請參考圖14，在軟體實施方式中，該設備配置裝置可

以包括獲取單元1401、識別單元1402和建立單元1403。其中：

獲取單元1401，使智慧設備在接收到任一使用者發送的近場通訊信號時，獲取所述近場通訊信號中包含的身份資訊；

識別單元1402，使所述智慧設備根據所述身份資訊對所述任一使用者進行身份識別；

建立單元1403，當判定所述任一使用者為所述智慧設備對應的管理使用者時，使所述智慧設備與所述任一使用者使用的電子設備建立近場通訊連接，供所述電子設備對所述智慧設備進行配置。

可選的，

還包括：上傳單元1404，使所述智慧設備將產生的隨機碼上傳至伺服器，以使所述伺服器產生與所述隨機碼相關的標準數位摘要，並將所述標準數位摘要發送至對所述智慧設備具有管理許可權的預設管理使用者，以作為所述預設管理使用者的身份資訊；其中，所述隨機碼還被記錄為所述智慧設備的本地隨機碼；

所述識別單元1402具體用於：所述智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並將所述本地數位摘要與所述近場通訊信號中作為所述身份資訊的待驗證數位摘要進行比較；其中，當所述待驗證數位摘要與所述本地數位摘要相匹配時，所述智慧設備判定所述任一使用者為所述智慧設備對應的管理使用者。

可選的，還包括：

更新單元1405，使所述智慧設備產生更新隨機碼並上傳至所述伺服器，以使所述伺服器對所述標準數位摘要進行更新；其中，所述更新隨機碼還被用於對所述本地隨機碼進行更新。

可選的，所述更新單元1405具體用於：

按照預定義週期產生所述更新隨機碼並上傳至所述伺服器；

或者，在完成配置操作後，產生所述更新隨機碼並上傳至所述伺服器。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦，電腦的具體形式可以是個人電腦、膝上型電腦、蜂窩電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件收發設備、遊戲控制台、平板電腦、可穿戴設備或者這些設備中的任意幾種設備的組合。

在一個典型的配置中，電腦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/或非易失性記憶體等形式，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暫存電腦可讀媒體(transitory media)，如調變的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其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。

這裡將詳細地對示例性實施例進行說明，其示例表示在圖式中。下面的描述涉及圖式時，除非另有表示，不同圖式中的相同數字表示相同或相似的要素。以下示例性實

施例中所描述的實施方式並不代表與本發明相一致的所有實施方式。相反，它們僅是與如申請專利範圍中所詳述的、本發明的一些方面相一致的裝置和方法的例子。

在本發明使用的術語是僅僅出於描述特定實施例的目的，而非旨在限制本發明。在本發明和申請專利範圍中所使用的單數形式的“一種”、“所述”和“該”也旨在包括多數形式，除非上下文清楚地表示其他含義。還應當理解，本文中使用的術語“和/或”是指並包含一個或多個相關聯的列出專案的任何或所有可能組合。

應當理解，儘管在本發明可能採用術語第一、第二、第三等來描述各種資訊，但這些資訊不應限於這些術語。這些術語僅用來將同一類型的資訊彼此區分開。例如，在不脫離本發明範圍的情況下，第一資訊也可以被稱為第二資訊，類似地，第二資訊也可以被稱為第一資訊。取決於語境，如在此所使用的詞語“如果”可以被解釋成為“在……時”或“當……時”或“回應於確定”。

以上所述僅為本發明的較佳實施例而已，並不用以限制本發明，凡在本發明的精神和原則之內，所做的任何修改、等同替換、改進等，均應包含在本發明保護的範圍之內。

【符號說明】

902：處理器

904：內部匯流排

906：網路介面

908：記憶體

910：非易失性記憶體

1001：發送單元

1002：識別單元

1003：請求單元

1004：接收單元

1005：添加單元

1102：處理器

1104：內部匯流排

1106：網路介面

1108：記憶體

1110：非易失性記憶體

1201：獲取單元

1202：返回單元

1203：更新單元

1302：處理器

1304：內部匯流排

1306：網路介面

1308：記憶體

1310：非易失性記憶體

1401：獲取單元

1402：識別單元

1403：建立單元

1404：上傳單元

1405：更新單元

201828162

【發明摘要】

【中文發明名稱】

設備配置方法及裝置、系統

【中文】

本發明提供一種設備配置方法及裝置、系統，該系統包括預設管理使用者的使用者設備、伺服器和智慧設備；其中：所述使用者設備向所述伺服器發送針對所述智慧設備的綁定請求，所述綁定請求用於指示所述伺服器對所述智慧設備進行綁定處理；所述伺服器在執行所述綁定處理的過程中，記錄所述管理使用者對所述智慧設備的管理許可權；所述智慧設備在接收到來自任一使用者的近場通訊信號時，識別所述任一使用者的使用者身份；當確定所述任一使用者為所述管理使用者時，與所述任一使用者的電子設備建立近場通訊連接，以供所述任一使用者對所述智慧設備進行配置。透過本發明的技術方案，可以基於軟體方式對設備進行配置，在簡化配置操作的同時，消除了實體按鍵存在的安全性隱患。

【指定代表圖】第(2)圖。

【代表圖之符號簡單說明】無

【特徵化學式】無

【發明申請專利範圍】

【第1項】

一種設備配置系統，其特徵在於，包括：預設管理使用者的使用者設備、伺服器和智慧設備；其中：

該使用者設備向該伺服器發送針對該智慧設備的綁定請求，該綁定請求用於指示該伺服器對該智慧設備進行綁定處理；

該伺服器在執行該綁定處理的過程中，記錄該管理使用者對該智慧設備的管理許可權；

該智慧設備在接收到來自任一使用者的近場通訊信號時，識別該任一使用者的使用者身份；當確定該任一使用者為該管理使用者時，與該任一使用者的電子設備建立近場通訊連接，以供該任一使用者對該智慧設備進行配置。

【第2項】

根據申請專利範圍第1項的系統，其中，

該伺服器記錄該管理使用者對該智慧設備的管理許可權，包括：該伺服器獲取該智慧設備產生並上傳的隨機碼，按照預設演算法產生與該隨機碼相關的標準數位摘要，並將該標準數位摘要與該智慧設備進行關聯記錄，使得該伺服器在接收到該使用者設備針對該智慧設備發送的配置請求時，向該管理使用者返回該標準數位摘要，以供該管理使用者對該智慧設備進行配置；其中，該隨機碼還被記錄為該智慧設備上的本地隨機碼；

該智慧設備識別該任一使用者的使用者身份，包括：

該智慧設備獲取該近場通訊信號中包含的待驗證數位摘要，並按照該預設演算法產生與記錄的本地隨機碼相關的本地數位摘要；其中，當該待驗證數位摘要與該本地數位摘要相匹配時，該智慧設備判定該任一使用者為該管理使用者。

【第3項】

一種設備配置方法，其特徵在於，包括：

使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示該智慧設備對該已登錄使用者進行身份識別；

根據該智慧設備對該近場通訊信號的回應，該使用者設備確定該智慧設備將該已登錄使用者判定為該智慧設備對應的管理使用者，並與該智慧設備建立近場通訊連接，以對該智慧設備進行配置。

【第4項】

根據申請專利範圍第3項的方法，其中，還包括：

該使用者設備向伺服器發送針對該智慧設備的配置請求，該配置請求用於指示該伺服器返回該智慧設備對應的標準數位摘要；

該使用者設備接收該伺服器返回的該標準數位摘要，以作為該已登錄使用者的身份資訊；其中，該標準數位摘要與該智慧設備預先產生並上傳的隨機碼相關，且該隨機碼還被記錄為該智慧設備上的本地隨機碼；

該使用者設備將該標準數位摘要作為該身份資訊添加

至該近場通訊信號中，以指示該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在該標準數位摘要與該本地數位摘要相匹配時，透過回應於該近場通訊信號，與該近場通訊信號的發送方設備建立近場通訊連接，供該發送方設備對該智慧設備進行配置。

【第5項】

根據申請專利範圍第4項的方法，其中，該智慧設備被綁定至預設團體；該配置請求中包含本端使用者的身份資訊，以指示該伺服器在該身份資訊匹配於該預設團體的管理使用者時，返回該智慧設備對應的標準數位摘要。

【第6項】

一種設備配置方法，其特徵在於，包括：

伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取該智慧設備對應的管理使用者的身份驗證資訊；

該伺服器向該預設使用者返回該身份驗證資訊，以由該預設使用者向該智慧設備發送包含該身份驗證資訊的近場通訊信號，該近場通訊信號用於指示該智慧設備根據該身份驗證資訊確定該預設使用者具有管理許可權，並與該近場通訊信號的發送方設備建立近場通訊連接，供該發送方設備對該智慧設備進行配置。

【第7項】

根據申請專利範圍第6項的方法，其中，該預設使用者為預設團體的管理使用者，且該智慧設備被預先綁定至

該預設團體。

【第8項】

根據申請專利範圍第6項的方法，其中，

該身份驗證資訊包括該智慧設備對應的標準數位摘要，該標準數位摘要與該智慧設備預先產生並上傳的隨機碼相關，且該隨機碼還被記錄為該智慧設備上的本地隨機碼；

其中，該近場通訊信號用於指示該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在該標準數位摘要與該本地數位摘要相匹配時，確定該預設使用者具有管理許可權。

【第9項】

根據申請專利範圍第8項的方法，其中：

該標準數位摘要為該隨機碼的數位摘要；

或者，該標準數位摘要為下述資訊中至少之一和該隨機碼的共同數位摘要：該智慧設備的啟動碼、該智慧設備的序號、該智慧設備的被綁定物件的標識資訊。

【第10項】

根據申請專利範圍第8項的方法，其中，還包括：

根據該智慧設備產生並上傳的更新隨機碼，該伺服器對記錄的該標準數位摘要進行更新；其中，該更新隨機碼還被該智慧設備用於對該本地隨機碼進行更新。

【第11項】

一種設備配置方法，其特徵在於，包括：

智慧設備在接收到任一使用者發送的近場通訊信號時，獲取該近場通訊信號中包含的身份資訊；

該智慧設備根據該身份資訊對該任一使用者進行身份識別；

當判定該任一使用者為該智慧設備對應的管理使用者時，該智慧設備與該任一使用者使用的電子設備建立近場通訊連接，供該電子設備對該智慧設備進行配置。

【第12項】

根據申請專利範圍第11項的方法，其中，

還包括：該智慧設備將產生的隨機碼上傳至伺服器，以使該伺服器產生與該隨機碼相關的標準數位摘要，並將該標準數位摘要發送至對該智慧設備具有管理許可權的預設管理使用者，以作為該預設管理使用者的身份資訊；其中，該隨機碼還被記錄為該智慧設備的本地隨機碼；

該智慧設備根據該身份資訊對該任一使用者進行身份識別，包括：該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並將該本地數位摘要與該近場通訊信號中作為該身份資訊的待驗證數位摘要進行比較；其中，當該待驗證數位摘要與該本地數位摘要相匹配時，該智慧設備判定該任一使用者為該智慧設備對應的管理使用者。

【第13項】

根據申請專利範圍第12項的方法，其中，還包括：

該智慧設備產生更新隨機碼並上傳至該伺服器，以使該伺服器對該標準數位摘要進行更新；其中，該更新隨機

碼還被用於對該本地隨機碼進行更新。

【第14項】

根據申請專利範圍第13項的方法，其中，該產生更新隨機碼並上傳至該伺服器，包括：

該智慧設備按照預定義週期產生該更新隨機碼並上傳至該伺服器；

或者，在完成配置操作後，該智慧設備產生該更新隨機碼並上傳至該伺服器。

【第15項】

一種設備配置裝置，其特徵在於，包括：

發送單元，使使用者設備向智慧設備發送包含已登錄使用者的身份資訊的近場通訊信號，以指示該智慧設備對該已登錄使用者進行身份識別；

識別單元，根據該智慧設備對該近場通訊信號的回應，使該使用者設備確定該智慧設備將該已登錄使用者判定為該智慧設備對應的管理使用者，並與該智慧設備建立近場通訊連接，以對該智慧設備進行配置。

【第16項】

根據申請專利範圍第15項的裝置，其中，還包括：

請求單元，使該使用者設備向伺服器發送針對該智慧設備的配置請求，該配置請求用於指示該伺服器返回該智慧設備對應的標準數位摘要；

接收單元，使該使用者設備接收該伺服器返回的該標準數位摘要，以作為該已登錄使用者的身份資訊；其中，

該標準數位摘要與該智慧設備預先產生並上傳的隨機碼相關，且該隨機碼還被記錄為該智慧設備上的本地隨機碼；

添加單元，使該使用者設備將該標準數位摘要作為該身份資訊添加至該近場通訊信號中，以指示該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在該標準數位摘要與該本地數位摘要相匹配時，透過回應於該近場通訊信號，與該近場通訊信號的發送方設備建立近場通訊連接，供該發送方設備對該智慧設備進行配置。

【第17項】

一種設備配置裝置，其特徵在於，包括：

獲取單元，使伺服器在接收到預設使用者針對預設智慧設備發送的配置請求時，獲取該智慧設備對應的管理使用者的身份驗證資訊；

返回單元，使該伺服器向該預設使用者返回該身份驗證資訊，以由該預設使用者向該智慧設備發送包含該身份驗證資訊的近場通訊信號，該近場通訊信號用於指示該智慧設備根據該身份驗證資訊確定該預設使用者具有管理許可權，並與該近場通訊信號的發送方設備建立近場通訊連接，供該發送方設備對該智慧設備進行配置。

【第18項】

根據申請專利範圍第17項的方法，其中，

該身份驗證資訊包括該智慧設備對應的標準數位摘要，該標準數位摘要與該智慧設備預先產生並上傳的隨機碼相關，且該隨機碼還被記錄為該智慧設備上的本地隨機

碼；

其中，該近場通訊信號用於指示該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並在該標準數位摘要與該本地數位摘要相匹配時，確定該預設使用者具有管理許可權。

【第19項】

根據申請專利範圍第18項的方法，其中，還包括：

更新單元，根據該智慧設備產生並上傳的更新隨機碼，使該伺服器對記錄的該標準數位摘要進行更新；其中，該更新隨機碼還被該智慧設備用於對該本地隨機碼進行更新。

【第20項】

一種設備配置裝置，其特徵在於，包括：

獲取單元，使智慧設備在接收到任一使用者發送的近場通訊信號時，獲取該近場通訊信號中包含的身份資訊；

識別單元，使該智慧設備根據該身份資訊對該任一使用者進行身份識別；

建立單元，當判定該任一使用者為該智慧設備對應的管理使用者時，使該智慧設備與該任一使用者使用的電子設備建立近場通訊連接，供該電子設備對該智慧設備進行配置。

【第21項】

根據申請專利範圍第20項的裝置，其中，

還包括：上傳單元，使該智慧設備將產生的隨機碼上

傳至伺服器，以使該伺服器產生與該隨機碼相關的標準數位摘要，並將該標準數位摘要發送至對該智慧設備具有管理許可權的預設管理使用者，以作為該預設管理使用者的身份資訊；其中，該隨機碼還被記錄為該智慧設備的本地隨機碼；

該識別單元具體用於：該智慧設備產生與記錄的本地隨機碼相關的本地數位摘要，並將該本地數位摘要與該近場通訊信號中作為該身份資訊的待驗證數位摘要進行比較；其中，當該待驗證數位摘要與該本地數位摘要相匹配時，該智慧設備判定該任一使用者為該智慧設備對應的管理使用者。

【第22項】

根據申請專利範圍第21項的裝置，其中，還包括：

更新單元，使該智慧設備產生更新隨機碼並上傳至該伺服器，以使該伺服器對該標準數位摘要進行更新；其中，該更新隨機碼還被用於對該本地隨機碼進行更新。