

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：96109913

※申請日期：96年03月22日

※IPC分類：G06Q 1/00 (2006.01)

H04L 9/32 (2006.01)

G06F 17/30 (2006.01)

一、發明名稱：

(中) 管理實體

(英) Managing an entity

二、申請人：(共 1 人)

1. 姓名：(中) 雷森公司

(英) RAYTHEON COMPANY

代表人：(中) 1. 愛德華 羅曼

(英) 1. ROMAN, EDWARD S.

地址：(中) 美國麻州瓦珊冬街八七〇號

(英) 870 Winter Street, Waltham, MA 02451-1449, U.S.A.

國籍：(中英) 美國 U.S.A.

三、發明人：(共 2 人)

1. 姓名：(中) 戴爾 瑞克曼

(英) RICKMAN, DALE M.

國籍：(中) 美國

(英) U.S.A.

2. 姓名：(中) 史蒂芬 馬利

(英) MARLEY, STEPHEN R.

國籍：(中) 美國

(英) U.S.A.

四、聲明事項：

◎本案申請前已向下列國家（地區）申請專利 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 美國 ; 2006/03/29 ; 11/392,246 有主張優先權

(1)

九、發明說明

【發明所屬之技術領域】

本發明係有關實體管理。

【先前技術】

通常已將實體管理與人員及物體相關聯。例如，對人員的管理可包括：將諸如護照或駕駛執照等的文件掃描到一系統中，或將該文件的文件編號輸入到該系統中，並自該系統接收該文件是否被認為是有效文件之一指示。在某些例子中，文件有效性的決定又決定了應對該人員應採取何種回應（例如，拒絕或允許進入一國家）。在其他的例子中，係將特定的行動與該文件相關聯。例如，如果決定護照是無效的，則行動將是拘留使用該護照的個人。

【發明內容】

在一觀點中，本發明是一種管理實體之方法。該方法包含下列步驟：使該實體的身分與名譽資料相關聯；以及根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯。該方法亦包含下列步驟：根據與該身分相關聯的該規則，而決定一回應。

在另一觀點中，本發明是一種管理實體之系統。該系統包含：具有名譽資料之一名譽資料庫、具有狀態資料之一狀態資料庫、以及組態被設定成與該名譽資料庫及該狀態資料庫互動之一規則引擎。該規則引擎之組態被設定成

(2)

根據狀態資料及與實體的身分相關聯的名譽資料而決定一回應。

在又一觀點中，本發明是一種物品。該物品包含一機器可讀取的媒體，用以儲存用來管理實體之可執行的指令。該等指令使一機器執行下列步驟：使實體的身分與名譽資料相關聯；根據狀態資料及名譽資料，而使一規則與該身分相關聯；以及根據該狀態資料及與該身分相關聯的該規則，而決定一回應。

在又一觀點中，本發明是一種管理進入一國家的人員之方法。該方法包含下列步驟：驗證進入該國家的一人員之身分；使該身分與名譽資料相關聯；根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯；以及根據與該身分相關聯的該規則，而決定一回應。

在又一觀點中，本發明是一種管理一系統的安全之方法。該方法包含下列步驟：驗證一人員或應用軟體之身分；使該身分與名譽資料相關聯；根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯；以及決定允許該身分使用的資料及服務。該方法亦可包含下列步驟：將一公開金鑰基礎結構（Public Key Infrastructure；簡稱 PKI）符記傳送回該人員或應用軟體。該人員或應用軟體可將該 PKI 符記用來要求服務或存取資料。否則，在沒有對應的 PKI 符記之情形下，該人員或應用軟體無法使用服務或將資料解密。

(3)

【實施方式】

本說明書中說明的是一種實體管理的創造性方法。雖然本說明書中述及的例子係被用於實體管理，但是本發明並不限於本說明書中述及的例子；更確切地說，可將本發明用於管理實體的任何系統或程序。

請參閱第 1 圖，一實體管理系統（Entity Management System；簡稱 EMS）（10）包含一身分驗證組件（12）、一名譽資料庫（16）、一狀態資料庫（20）、一規則引擎（24）、以及一回應模組（28）。如將於下文中更進一步說明的，可將 EMS（10）用來決定利用回應模組（28）對實體作出的回應。回應模組（28）可提供：對實體資格的授予、及（或）將對該實體執行的一列表之行動。該實體可以是人員、動物、有機體（例如，病毒）、物體、系統、或以上各項之任何組合。

身分驗證組件（12）驗證實體的身分。例如，該實體可以是試圖進入一安全設施的一人員。在另一例子中，該實體可以是進入一國家且正在被海關處理的一運送包裝。在又一例子中，該實體可以是進入一國家的牛。在又一例子中，該實體可以是試圖存取一第二系統之一第一系統（例如，一應用軟體）。在另一例子中，該實體可以諸如被偵測到的一病毒等的一有機體。在其他例子中，實體可以是諸如個人資料助理（Personal Data Assistant；簡稱 PDA）、細胞式電話、或無線電等的被用來存取一系統之裝置。在又一例子中，實體可以是一信用卡。

(4)

身分驗證組件（12）包含一身分處理器（32）及一身分資料庫（36）。身分資料庫（36）包含被用來識別實體的身分資料。該身分資料可以是生物特徵資料、運送標籤、以及護照掃描影像等的身分資料。使該身分資料與用來識別身分的唯一識別碼相關聯。例如，可使一單一的指紋掃描與一唯一識別碼相關聯。身分處理器（32）自規則引擎（24）接收實體資料，並利用身分資料庫（36）中之身分資料決定該實體的身分。

在一例子中，係在諸如登記程序等的一初始化程序期間中儲存該身分資料。例如，將在該系統中登記要求簽證的一外國旅客。一實體後續對 EMS（10）的存取涉及將該後續存取期間之實體資料與身分資料庫（36）中儲存的身分資料比較。例如，當該外國旅客抵達移居地時進行比較。

名譽資料庫（16）包含與一或多個身分有關的歷史性資料。唯一識別碼使歷史性資料與身分相關聯。該歷史性資料可包括該身分的過去移居資料。例如，該歷史性資料可包括個人在一國家的逾期居留（亦即，在一國家居留超過簽證授權的時間）資料。該歷史性資料亦可包括該身分的過去行動資料。例如，過去行動可包括受懲罰的歷史或暴動集會的參與。在另一例子中，過去行動可包括該身分進入一國家的機場或港口以及該身分的進入次數。名譽資料庫（16）亦可包括身分的關係資料。例如，該關係資料可包括與其他個人、團體（例如，家庭、服務類型、組織

(5)

)、以興趣為基礎的社群（例如，地理區）、角色、以及應用等的其他實體之聯繫。名譽資料庫（16）可進一步包括推薦資料。例如，該推薦資料可包括第三方對該身分所採取的一行動（例如，同意該身分的存取）之推薦。

名譽資料庫（16）亦可包含第三方確認。例如，於登記大量的實體時，讓該等實體自己登記，但在完成登記之前，先由可信賴之第三方確認該等實體，此種方式可能是更有效率的。例如，要求進入一建築物或使用一服務的僱員可輸入其本身的資訊，但是在完成該登記之前，將先由主管安全的部門或該等僱員的經理確認其資訊及名譽。在另一例子中，可由一願意保證一託運人的一第三方獨立公司證實該託運人的名譽。在取得極機密結關許可的又一例子中，第三方確認可以是政府業已執行詳細的背景檢查之一跡證。

名譽資料庫（16）可以是一資料庫、或分佈在寬廣的地理區（例如，跨越一洲或數洲）且被一網路連接的一些資料庫之一組合。在一例子中，可將名譽資料庫（16）設於一位置。在另一例子中，名譽資料庫（16）可包含被設置在不同位置的一些部分。名譽資料庫（16）可以是單一電腦或一組電腦的一部分。

在其他例子中，一完整的名譽資料庫可不被包含在EMS（10）中。例如，可能需要查詢一外部的資料庫（圖中未示出），以便存取名譽資料。更具體而言，在將EMS（10）用來管理進入一國家的旅客之例子中，可核對

(6)

遺失／被偷護照的一 INTERPOL 資料庫。

狀態資料庫 (20) 包含狀態資料。狀態資料可指示 EMS (10) 的操作環境或該操作環境的一部分。例如，該狀態資料可以是一威脅預警等級 (threat advisory level) 或安全警示。該狀態資料可進一步指示未來的環境為何。例如，在一指定的未來日期，威脅預警等級將自高變成低。在另一例子中，該狀態資料可指示使用 EMS (10) 的一設施之作業小時數。

在一例子中，狀態資料可以是將會影響到一組大量的總體 (而不是特定的個人或品目) 之任何資訊。例如，安全漏洞可能會使個人資訊遺失 (例如，遺失個人識別碼 (Personal Identification Number; 簡稱 PIN))。在另一例子中，狀態資料可包括天氣資料。在又一例子中，狀態資料可包括建築物或船舶的溫度資料。

規則引擎 (24) 包含一實體輸入介面 (42)、一控制器 (44)、一危險處理器 (45)、一危險資料庫 (46)、一規則處理器 (47)、以及具有規則之一規則資料庫 (48)。實體輸入介面 (42) 自實體接收資訊，以便決定實體的身分。在一例子中，實體輸入介面 (42) 是一文件讀取器，該文件讀取器掃描文件 (例如，護照、駕駛執照、以及運送標籤等的文件) 上的條碼。在另一例子中，實體輸入介面 (42) 是生物特徵掃描器，用以掃描諸如指紋、虹膜、聲音、以及去氧核糖核酸 (DNA) 等的生物特徵資料。在又一例子中，實體輸入介面 (42) 是用來讀取安全加

(7)

密金鑰之一電腦程式。

在其他例子中，實體輸入介面（42）包含一射頻識別（Radio Frequency Identification；簡稱RFID）讀取器，用以讀取RFID標籤。在其他例子中，實體輸入介面（42）可接收使用者名稱及密碼。在又一例子中，實體輸入介面（42）可以是在離開位置上將貨櫃的內容物成像之一裝置，且另一實體輸入介面（圖中未示出）可在到達位置上將貨櫃成像。驗證組件（12）比較該貨櫃是同一貨櫃以及該貨櫃在沿途中並未被篡改的兩個影像，而驗證該貨櫃。

控制器（44）控制外部及內部組件的資訊進出規則引擎（24）的流程。例如，控制器（44）將實體輸入介面（42）所接收的實體資料傳送到身分驗證組件（12）。控制器（44）也存取諸如名譽資料庫（16）及狀態資料庫（20）等的資料庫。控制器（44）也控制危險處理器（45）及規則處理器（47）。控制器（44）將用來指示實體與EMS（10）間之互動之一回應之一信號傳送到回應模組（28）。

危險處理器（45）使名譽資料庫（16）中之一身分的名譽資料與危險資料庫（46）中儲存的危險準則相關聯。在一例子中，危險處理器（45）根據與該身分相關聯的名譽資料而指定一危險分數。

規則處理器（47）根據來自狀態資料庫（20）的狀態資料、以及來自名譽資料庫（16）的與該身分相關聯之名

(8)

譽資料，而利用規則資料庫（48）中之規則決定回應模組（28）之一回應。在一例子中，一身分進入有港口 A 及港口 B 的兩個入境港口之一國家。名譽資料可包括進入一國家及入境港口之時間。與一身分相關聯的名譽資料指示該個人過去在每個工作日進入港口 A。然後，該身分於夜晚進入港口 B。規則引擎（24）將偵測行為的改變，並使用狀態資料而將一規則（例如，阻止該身分）與該身分相關聯。例如，指示一高威脅等級的狀態資料可要求阻止且搜查該身分，而指示一低威脅等級的狀態資料可不要求阻止且詢問該身分。狀態資料改變的另一例子可包括將影響到情報資訊的存取碼，因而增加了更多監督的規則。

回應模組（28）亦可提供 EMS（10）的使用者將進行的行動。例如，如果在一國家的移民中心使用 EMS（10），則回應模組（28）可詢問身分進一步的探索式問題。在另一例子中，回應模組（28）可提供諸如對一電腦的存取以及對進入一限制區的授權等的權利或特權。

在某些例子中，回應模組（28）可提供顯示結果（例如，電腦螢幕上的訊息），或者回應模組（28）可控制一實體裝置。例如，在 EMS（10）被用來控制自飛機卸下的行李之例子中，回應模組（28）可將高危險的旅行袋輸送到一分離的區域，以便進行詳細的檢查。如果 EMS（10）被用於登記過的旅行計劃，則回應模組（28）可開啓入口，以便讓旅客進入，或將旅客轉送到一地方，以便進行第二檢查。

(9)

在某些例子中，EMS (10) 可不包含回應模組 (28) 。例如，如果在一應用使用的軟體中實施 EMS (10) ，則可將回應 (例如，一訊息) 直接傳送回該應用。

請參閱第 2 圖，用來管理實體的一例示程序是程序 (50) 。程序 (50) 在步驟 (52) 中接收實體資料。例如，實體輸入介面 (42) 接收將被用來決定實體的身分之實體資料。例如，該實體出示一文件 (例如，護照及駕駛執照等的文件) ，且該文件被掃描到實體輸入介面 (42) 中。在另一例子中，自該實體讀取生物特徵資料 (例如，指紋掃描、聲紋掃描、虹膜掃描、及 DNA 等的生物特徵資料) ，且該生物特徵資料被下載到實體輸入介面 (42) 。在又一例子中，係經由一通訊鏈路將一安全加密金鑰提供給實體輸入介面 (42) 。在又一例子中，掃描被貼附在該實體的運送標籤。

程序 (50) 在步驟 (54) 中利用實體資訊驗證身分。例如，控制器 (44) 將實體資料傳送到身分驗證組件 (12)) 。身分處理器 (32) 將該實體資料與身分資料庫 (36) 中儲存的身分資料比較。本發明身分處理器 (32) 利用實體輸入介面 (42) 所掃描的指紋搜尋該身分資料庫，以便找出一匹配的指紋、或在某一公差下匹配的指紋。將該匹配的指紋與用來將該實體識別為一特定身分的一唯一識別碼相關聯。

程序 (50) 在步驟 (56) 中將該唯一識別碼傳輸到規則引擎 (24) 。在一例子中，控制器 (44) 自身分驗證組

件（12）擷取該唯一識別碼。在另一例子中，身分驗證組件（12）將該唯一識別碼傳送到控制器（44）。

程序（50）在步驟（62）中傳輸與該唯一識別碼相關聯的名譽資料。例如，控制器（44）利用該唯一識別碼自名譽資料庫（16）擷取名譽資料。在另一例子中，當名譽資料庫（16）是分散式資料庫時，控制器（44）將一起始查詢傳送到名譽資料庫（16）的一部分。名譽資料庫（16）產生對名譽資料庫（16）的其餘部分之查詢，等候來自名譽資料庫（16）的其餘部分之回應，並將一合併的回應傳送回規則引擎（24）。

程序（50）在步驟（66）中建立該名譽資料之關聯性。例如，控制器（44）將與一唯一識別碼相關聯的名譽資料傳送到危險處理器（45）。危險處理器（45）應用來自危險資料庫（46）的危險準則，並指定用來標示危險的一數字分數，並指定用來標示危險的一數字分數（危險分數）。下文中將參照第 3 圖而說明建立名譽資料的關聯性之另一例子。

程序（50）在步驟（72）中傳輸狀態資料。例如，控制器（44）自狀態資料庫（20）擷取狀態資料。在另一例子中，狀態資料庫（20）將狀態資料傳送到控制器（44）。在其他例子中，可以定期之方式或在狀態資料發生改變時進行狀態資料的傳輸。

程序（50）在步驟（76）中根據狀態資料以及與該身分相關聯的名譽資料，而使該等規則與該身分相關聯。例

(11)

如，該控制器將相關聯的名譽資料及狀態資料傳送到規則處理器（47）。規則處理器（47）應用來自規則資料庫（48）之規則。下文中將參照第4圖而說明建立規則的關聯性之一例子。

程序（50）在步驟（82）中根據該等規則之關聯性而決定一回應。例如，控制器（44）將一信號傳送到回應模組（28），以便執行一回應。程序（50）在步驟（86）中更新名譽資料庫。例如，在名譽資料庫（16）接收到控制器（44）發出的一實體正在步驟（56）中與EMS（10）互動之通知之後，即更新名譽資料庫（16）。例如，每當一旅客進入一國家時，即產生一新的歷史性記錄。

請參閱第3及4圖，對此項技術具有一般知識者將可了解：有儲存資料、呈現資料、以及建立EMS（10）內的資料之關聯性之各種方式。在將EMS（10）用於接納來自外國的旅客的一機場一例子中，可指定一分數，並連同一危險等級而呈現該分數，而執行名譽資料的關聯性之建立（第2圖中之步驟（66）。例如，可將一公式（危險準則）用來將一分數指定給與該身分相關聯的名譽資料，且進一步使該分數與一危險等級相關聯。如果該身分因該名譽資料而出現在一警戒清單，且具有與恐怖組織之類的組織間之關聯性，則可指定代表“高危險”實體的“11”或更高的一分數。如果該身分因該名譽資料而係為新的旅客或未知的旅客，則可指定代表“中度危險”實體的“6”至“10”間之一分數。如果該身分因該名譽資料而係為經常性旅客且並未

(12)

出現在任何清單中，則可使代表“低危險”實體的小於“5”之一分數與該身分相關聯。

繼續前段所述的例子，可以一表（100）代表規則的關聯性之建立（第2圖之步驟（76）），該表（100）具有用來代表來自名譽資料的危險等級（例如，第3圖所示之危險等級）之一些行（110）、以及用來代表來自狀態資料的狀態等級（例如，狀態1、狀態2、以及狀態3）之一些列（120）。狀態1可代表低威脅等級，狀態2可代表中度威脅等級，且狀態3可代表高威脅等級。使每一列／行之組合與一規則（例如，規則1、規則2、規則3、規則4、以及規則5）相關聯。規則1可以是讓該身分進入該國家。規則2可以用一組問題詢問該身分。規則3可以是搜查該身分的攜帶物品。規則4可以是搜查該身分的身體。規則5可以是逮捕該身分。因此，使用表（100）時，規則引擎（24）可採用狀態資料以及與該身分相關聯的名譽資料，以便使一規則與該身分相關聯，而決定一回應（例如，第2圖之步驟（82））。

可將其他的例子用來建立名譽資料之關聯性。在處理進入一國家的旅客之一例子中，在旅客已進入該國家且準時離開有了某些次數（例如，大於10次）之前，該旅客可能無法取得低危險分數。在另一例子中，經常旅行且不曾有過逾期居留的旅客將被評定為低危險。在又一例子中，出現在一警戒清單或具有遺失或被偷的護照時，可自動改變與該旅客相關的規則。

(13)

在進入一國家的貨物之一例子中，關聯性將考慮到託運人將貨物進口到該國家的年數、該貨物被檢驗的次數、及（或）招遇到問題的次數。除了託運人的歷史性資料之外，可根據被運送的品目之類型而計算危險等級。例如，可將低危險指定給紡織品，而至少將中度危險自動指定給電子產品，且必然將高危險指定給放射性材料，且放射性材料將接受搜查。

可以一線上拍賣模型中舉例說明建立名譽資料的關聯性之另一例子，其中在該模型中，人們係根據在其間進行的交易而相互評分。例如，可將高危險指定給只有與系統有幾次交易的某些人。在另一例子中，可將高危險指定給受到許多負面評論的人。

對此項技術具有一般知識者將可了解：可將 EMS（10）應用於本說明書中述及的例子以外之其他例子。

在一例子中，可將 EMS（10）用於一國家的邊境，以便處理進入該國家的牛。在該例子中，身分驗證可包括耳標（ear tag）的讀取。名譽資料可包括牛移動的歷史性資料。牛移動的歷史性資料可包括在牛的過去移動期間與該等牛互動的有哪些其他的牛，其中包括被識別有狂牛症的那些其他的牛。名譽資料亦可包括牛託運人的名譽資料、或提供牛的國家的名譽資料。例如，來自不曾發生狂牛症的國家的牛將比來自最近爆發狂牛症的國家的牛有較低的危險。此外，狀態資料可以是諸如最今發生狂牛症的肉品業之狀態。

(14)

在另一例子中，可將 EMS (10) 用於處理經由一入境港口處理的運送包裝。在該例子中，身分驗證可包括讀取運送標籤。在另一例子中，身分驗證可包括對包裝的內容物之掃描。可使名譽資料與託運人相關聯（例如，託運人是否有良好聲譽）。在該例子中，可將 EMS (10) 用來決定何種回應對所接收的每一包裝是適宜的。名譽資料可包括原產地國家。例如，來自以知道有毒品走私的國家之包裝將有比並無上述問題的國家之包裝有較高危險。

在又一例子中，可將 EMS (10) 用於具有一主伺服器以及一些無線電之一通訊系統中。名譽資料可包括每一無線電與該伺服器互動的時間點及持續時間。在該例子中，可將 EMS (10) 用來識別長時間期間並未與該伺服器互動（因而可能表示被敵人損壞）的那些無線電。EMS (10) 可加入額外的安全協定，用以驗證無線電的使用者是否為友好的。在另一例子中，名譽資料可包括先前被存取的資料及被要求的服務，並將該等過去的狀況與現行的或最近的要求比較，以便偵測到改變。改變可表示較高的危險。

在又一例子中，諸如退伍軍人管理局（Veterans Administration；簡稱 VA）等的美國政府機構可使用 EMS (10)。尤其，退伍軍人根據其兵役的期間（例如，平時或戰時）以及其兵役的持續時間而具有不同福利的資格。可將 EMS (10) 用來確保將適當的福利授予每一退伍軍人。該等福利也根據法律的改變而不時改變。名譽資料亦可包括退伍軍人申請福利的地方、以及所要求的福利類型

。例如，新類型的福利或在多個退伍軍人管理局辦公室所作的要求可能指示一危險，且將引起所適用的不同法規。狀態改變可包括退伍軍人記錄的遺失或被偷。

在又一例子中，EMS（10）可用於信用卡，不只是用於購買的允許／拒絕，且亦決定是否應改變信用額度上限。在另一例子中，如果大量的銀行信用卡 PIN 被偷，則可將 EMS（10）用來偵測具有狀態資料改變之不平常的活動（使用名譽資料），以便使一組大量的銀行信用卡失效。

第 5 圖示出可被用來執执行程序（50）之一電腦（200）。電腦（200）包含一處理器（202）、一揮發性記憶體（204）、以及一非揮發性記憶體（206）（例如，硬碟）。非揮發性記憶體（206）包含一作業系統（210）、名譽資料（212）、規則資料（216）、狀態資料（218）、以及被用來自揮發性記憶體（204）執行以便執执行程序（50）之電腦指令（214）。電腦（200）亦包含一圖形使用者介面（Graphical User Interface；簡稱 GUI）（203）、一輸入介面（205）、以及一輸出介面（207）。使用者可將 GUI（203）用來輸入資料（例如，護照號碼等的實體資料）及接收處理器（202）所傳送的資料（例如，指令等的回應模組（28））。輸入介面（205）可以用來接收實體資料的掃描器及生物特徵分析儀等的輸入介面（例如，第 1 圖所示之實體輸入介面（42））。輸出介面（207）可以用來執行回應的任何裝置。例如，輸出介面（207）可被用來互動並解除門禁而許可進入，或被用來

經由一網路而傳送一鑑定金鑰。

程序（50）並不限於配合第5圖所示之硬體及軟體使用；可將程序（50）應用於任何運算或處理環境，且配合可執行電腦程式的任何類型之機器或機器組而使用。可以硬體、軟體、或以上兩者的組合實施程序（50）。可以在可程式電腦／機器中執行的電腦程式實施程序（50），而該等可程式電腦／機器分別包含一處理器、一儲存媒體或該處理器可讀取的其他製品（其中包括揮發性及非揮發性記憶體、及（或）儲存元件）、至少一輸入裝置、以及一或多個輸出裝置。可使用一輸入裝置以執行程序（50），並產生輸出資訊，而將程式碼應用於被輸入的資料。

可經由一電腦程式產品（亦即，在一資訊載體（例如，機器可讀取的儲存裝置或被傳播的信號）中具體實施之一電腦程式）而至少部分地實施該系統，以便被資料處理裝置（例如，可程式處理器、電腦、或多個電腦）執行，或控制資料處理裝置之作業。可以一高階程序或物件導向程式語言實施每一此類程式，以便與一電腦系統通訊。然而，可以組合語言或機器語言實施該等程式。該語言可以是一編譯式或直譯式語言，且可以其中包括作為獨立程式或模組、元件、次常式、或適用於運算環境的其他單位之任何形式部署該語言。可將一電腦程式部署成在一場所或分佈在個場所且由一通訊網路互連之一個電腦或多個電腦中執行。可在一儲存媒體或裝置（然而，唯讀光碟、硬碟、或軟碟）中儲存電腦程式，而一般用途或特殊用途電腦

可讀取該電腦程式，以便在該儲存媒體或裝置被該電腦讀取時，可設定該電腦的組態並操作該電腦，而執行程序（50）。亦可將程序（50）實施為一機器可讀取的儲存媒體，並以一電腦程式設定該程序（50）之組態，而當執行程序（50）時，該電腦程式中之指令將使該電腦根據程序（50）而操作。

本發明所述之程序不限於本說明書中述及的特定實施例。例如，該等程序不限於第 2 圖所示之特定處理順序。更確切地說，可視需要而重新安排第 2 圖所示步驟中之任何步驟的順序，合併或移除任何步驟，或者以平行或接續之方式執行任何步驟，以便獲致前文所述之結果。可合併控制器（44）、危險處理器（45）、以及規則處理器（47），以便形成一處理器。可合併危險資料庫（46）及規則資料庫（48），以便形成一資料庫。

本發明所述之該系統不限於配合前文所述之硬體及軟體而使用。可以數位電子電路、電腦硬體、韌體、軟體、或以上各項的組合實施該系統。

可以用來執行一或多個電腦程式以執行該系統的功能之一或多個可程式處理器執行與該系統的實施相關聯之方法步驟。可將該系統的全部或部分實施為一特殊用途邏輯電路（例如，客戶端可程式閘陣列（Field-Programmable Gate Array；簡稱 FPGA）及（或）一特定應用積體電路（Application Specific Integrated Circuit；簡稱 ASIC）。

適於執行電腦程式的處理器包括諸如一般用途及特殊用途微處理器、以及任何種類的數位電腦中之任何一或多個處理器。一般而言，處理器將自唯讀記憶體或隨機存取記憶體或以上兩者接收指令及資料。一電腦的元件包含用來執行指令之一處理器、以及用來儲存指令及資料之一或多個記憶體裝置。

可合併本發明所述不同實施例的元件，以便形成前文中並未明確述及的其他實施例。本說明書中並未明確述及的其他實施例也是在最後申請專利範圍之範圍內。

【圖式簡單說明】

第 1 圖是一實體管理系統之一功能圖。

第 2 圖是用來管理實體的一程序之一流程圖。

第 3 圖示出使名譽資料與身分相關聯的一例子。

第 4 圖示出使規則與身分相關聯的一例子。

第 5 圖是可用來實施第 2 圖所示程序的一電腦系統之一方塊圖。

【主要元件符號說明】

10：實體管理系統

12：身分驗證組件

16：名譽資料庫

20：狀態資料庫

24：規則引擎

- 28 : 回應模組
- 32 : 身分處理器
- 36 : 身分資料庫
- 42 : 實體輸入介面
- 44 : 控制器
- 45 : 危險處理器
- 46 : 危險資料庫
- 48 : 規則資料庫
- 100 : 表
- 110 : 行
- 120 : 列
- 200 : 電腦
- 202 : 處理器
- 204 : 揮發性記憶體
- 206 : 非揮發性記憶體
- 210 : 作業系統
- 212 : 名譽資料
- 216 : 規則資料
- 218 : 狀態資料
- 214 : 電腦指令
- 203 : 圖形使用者介面
- 205 : 輸入介面
- 207 : 輸出介面

五、中文發明摘要

發明之名稱：管理實體

在一觀點中，本發明是一種管理實體之方法。該方法包含下列步驟：使該實體的身分與名譽資料相關聯；以及根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯。該方法亦包含下列步驟：根據與該身分相關聯的該規則，而決定一回應。

六、英文發明摘要

發明之名稱：Managing an entity

In one aspect the invention is a method of managing an entity. The method includes associating an identity of an entity to reputation data, associating a rule to the identity based on status data and the reputation data associated with the identity. The method also includes determining a response based on the rule associated with the identity.

(1)

十、申請專利範圍

1. 一種管理實體之方法，包含下列步驟：

使該實體的身分與名譽資料相關聯；

根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯；以及

根據與該身分相關聯的該規則，而決定一回應。

2. 如申請專利範圍第 1 項之方法，進一步包含下列步驟：驗證該實體的身分。

3. 如申請專利範圍第 2 項之方法，其中驗證身分之該步驟包含下列步驟：驗證一生命形式的身分。

4. 如申請專利範圍第 2 項之方法，其中驗證身分之該步驟包含下列步驟：驗證一物體的身分。

5. 如申請專利範圍第 2 項之方法，其中驗證身分之該步驟包含下列步驟：驗證一系統的身分。

6. 如申請專利範圍第 1 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與該身分的一先前行動相關聯。

7. 如申請專利範圍第 1 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與一組實體相關聯。

8. 如申請專利範圍第 1 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與一地理位置相關聯。

9. 如申請專利範圍第 1 項之方法，其中決定回應之

(2)

該步驟包含下列步驟：決定一行動。

10. 如申請專利範圍第 1 項之方法，其中決定回應之該步驟包含下列步驟：決定該身分之權利。

11. 一種管理實體之系統，包含：

具有名譽資料之一名譽資料庫；

具有狀態資料之一狀態資料庫；以及

組態被設定成與該名譽資料庫及該狀態資料庫互動之一規則引擎，該規則引擎之組態被設定成根據狀態資料及與實體的身分相關聯的名譽資料而決定一回應。

12. 如申請專利範圍第 11 項之系統，進一步包含組態被設定成被連接到該規則引擎之一身分驗證組件，且其中該身分驗證組件驗證該實體的身分。

13. 如申請專利範圍第 12 項之系統，其中該實體包含一生命形式。

14. 如申請專利範圍第 12 項之系統，其中該實體包含一物體。

15. 如申請專利範圍第 12 項之系統，其中該實體包含一系統。

16. 如申請專利範圍第 11 項之系統，其中該規則引擎使該身分與該身分的一先前行動相關聯。

17. 如申請專利範圍第 11 項之系統，其中該規則引擎使該身分與一組實體相關聯。

18. 如申請專利範圍第 11 項之系統，其中該規則引擎之組態被設定成使該身分與一地理位置相關聯。

(3)

19. 如申請專利範圍第 11 項之系統，其中組態被設定成決定回應之該規則引擎包含組態被設定成決定一行動之規則引擎。

20. 如申請專利範圍第 11 項之系統，其中組態被設定成決定回應之該規則引擎包含組態被設定成決定該身分之權利之規則引擎。

21. 一種物品，該物品包含一機器可讀取的媒體，用以儲存用來管理實體之可執行的指令，該等指令使一機器執行下列步驟：

使該實體的身分與名譽資料相關聯；

根據狀態資料及名譽資料，而使一規則與該身分相關聯；以及

根據該狀態資料及與該身分相關聯的該規則，而決定一回應。

22. 如申請專利範圍第 21 項之物品，進一步包含使該機器驗證該實體的身分之指令。

23. 如申請專利範圍第 22 項之物品，其中使該機器驗證身分之該等指令包含使該機器驗證一生命形式的身分之指令。

24. 如申請專利範圍第 22 項之物品，其中使該機器驗證身分之該等指令包含使該機器驗證一物體的身分之指令。

25. 如申請專利範圍第 22 項之物品，其中使該機器驗證身分之該等指令包含使該機器驗證一系統的身分之指

(4)

令。

26. 如申請專利範圍第 21 項之物品，其中使該機器使該身分與名譽資料相關聯之該等指令包含使該機器使該身分與該身分的一先前行動相關聯之指令。

27. 如申請專利範圍第 21 項之物品，其中使該機器使該身分與名譽資料相關聯之該等指令包含使該機器使該身分與一組實體相關聯之指令。

28. 如申請專利範圍第 21 項之物品，其中使該機器使該身分與名譽資料相關聯之該等指令包含使該機器使該身分與一地理位置相關聯之指令。

29. 如申請專利範圍第 21 項之物品，其中使該機器決定回應之該等指令包含使該機器決定一行動之指令。

30. 如申請專利範圍第 21 項之物品，其中使該機器決定回應之該等指令包含使該機器決定該身分之權利之指令。

31. 一種管理進入一國家的人員之方法，包含下列步驟：

驗證進入該國家的一人員之身分；

使該身分與名譽資料相關聯；

根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯；以及

根據與該身分相關聯的該規則，而決定一回應。

32. 如申請專利範圍第 31 項之方法，進一步包含下列步驟：驗證該人員之身分。

(5)

33. 如申請專利範圍第 31 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與該人員的一先前行動相關聯。

34. 如申請專利範圍第 31 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與一組人員相關聯。

35. 如申請專利範圍第 31 項之方法，其中使該身分與名譽資料相關聯之該步驟包含下列步驟：使該身分與一地理位置相關聯。

36. 如申請專利範圍第 31 項之方法，其中決定回應之該步驟包含下列步驟：決定一行動。

37. 如申請專利範圍第 31 項之方法，其中決定回應之該步驟包含下列步驟：決定該身分之權利。

38. 一種管理一系統的安全之方法，包含下列步驟：
驗證一實體之身分；

使該身分與名譽資料相關聯；

根據狀態資料及與該身分相關聯的名譽資料，而使一規則與該身分相關聯；以及

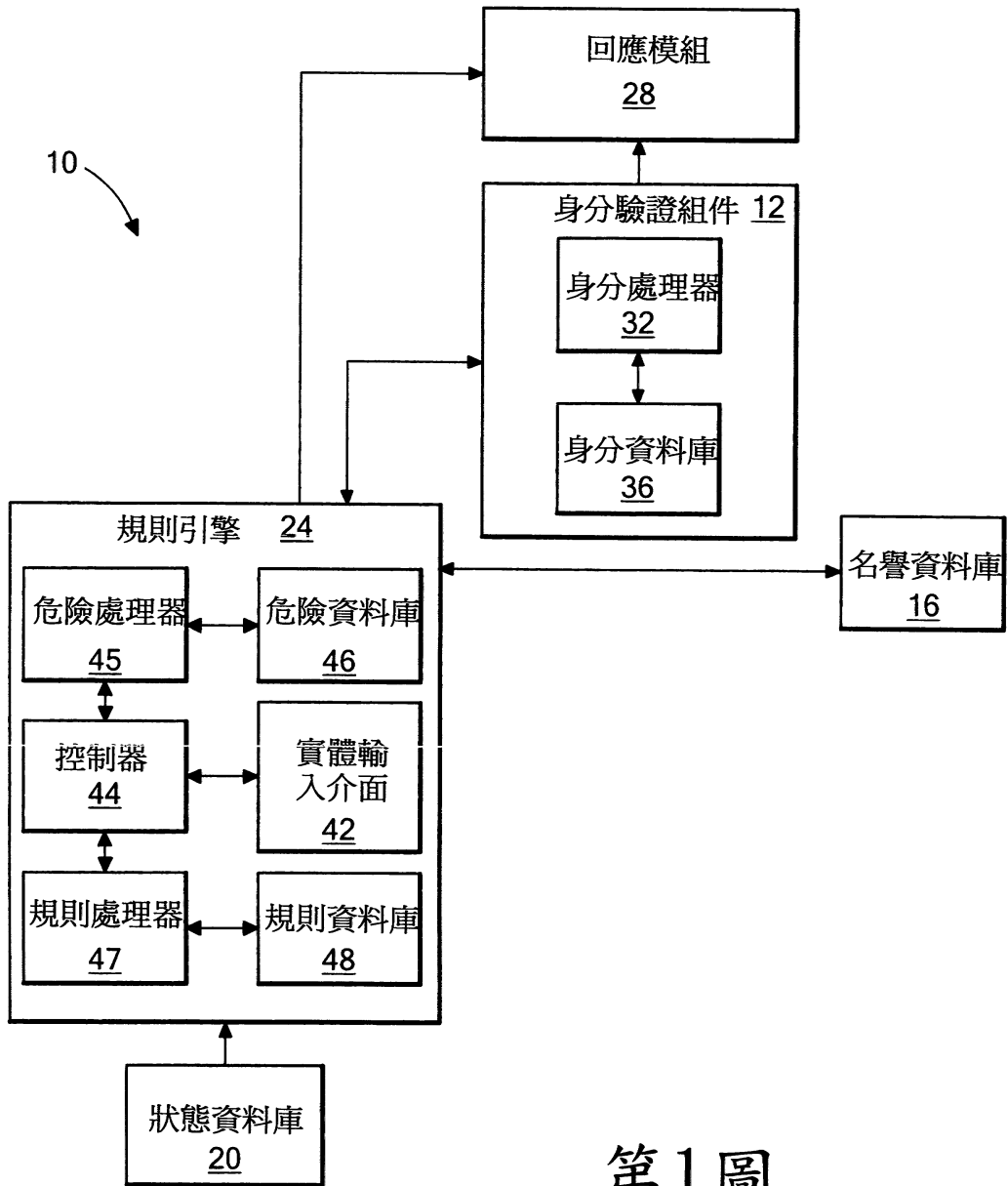
決定允許該身分使用的資料及服務。

39. 如申請專利範圍第 38 項之方法，其中驗證一實體之身分之該步驟包含下列步驟：驗證一人員。

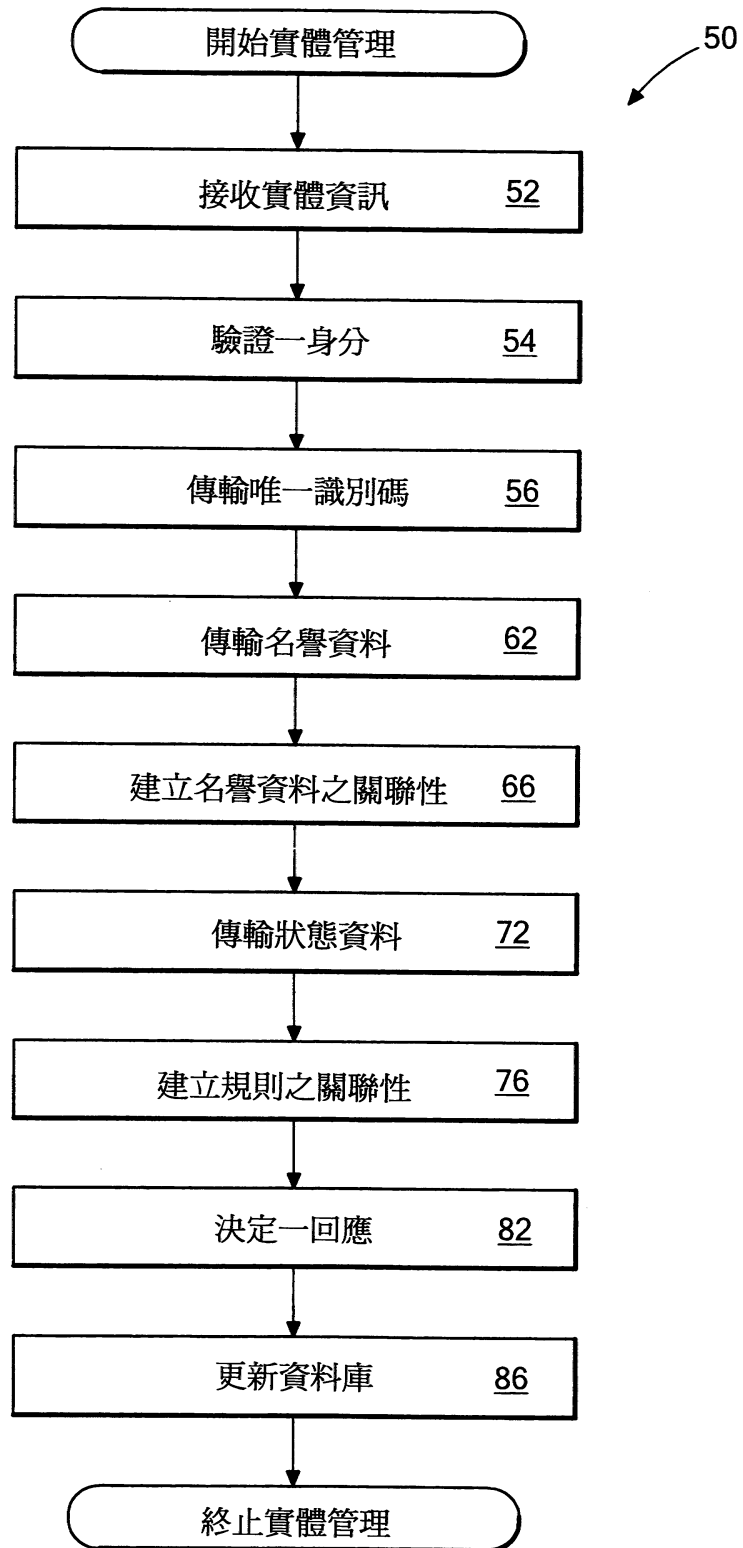
40. 如申請專利範圍第 38 項之方法，其中驗證一實體之身分之該步驟包含下列步驟：驗證一應用軟體之身分。

(6)

41. 如申請專利範圍第 38 項之方法，進一步包含下列步驟：將一公開金鑰基礎結構（PKI）符記傳送回該實體。



第1圖



第2圖

七、指定代表圖：

(一)、本案指定代表圖為：第(2)圖。

(二)、本代表圖之元件代表符號簡單說明：

10：實體管理系統	12：身分驗證組件
16：名譽資料庫	20：狀態資料庫
24：規則引擎	28：回應模組
32：身分處理器	36：身分資料庫
42：實體輸入介面	44：控制器
45：危險處理器	46：危險資料庫
47：規則處理器	48：規則資料庫

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無