申請日期	86. 1. 29
案號	86100985
類別	Int. Cl.[6] G06F 3/00, 13/00

（以上各欄由本局填註）

公告本 316963 C4

316963

發明 ~~新型~~ 專利說明書

一、發明 ~~新型~~ 名稱	中文	經由在列印節點上之使用者辨識以防止揭露之裝置及方法
	英文	APPARATUS AND METHOD FOR PREVENTING DISCLOSURE THROUGH USER-AUTHENTICATION AT A PRINTING NODE
二、發明 ~~創作~~ 人	姓名	1.德瑞克 L. 戴維斯 2.利昂 史密斯
	國籍	均美國
	住、居所	1.美國亞歷桑納州鳳凰城東德塞特派路4509號 2.美國亞歷桑納州皇后奎克市凡德阿若悠23412號
三、申請人	姓名（名稱）	美商英特公司
	國籍	美國
	住、居所（事務所）	美國加州聖塔卡拉瓦市米遜大學路2200號
	代表人姓名	F．湯姆士．當烈二世

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

美　國（地區）　申請專利，申請日期：1995.12.19　案號：594,843　，□有　□無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（1）

相關發明參考

本發明之發明人之一亦提出美國專利的合併申請案，標題爲"提供安全通訊之裝置及方法"(Apparatus and Method for Providing Secured Communications)（案號：08/251,486）；"一硬體媒介之移動軟體許可"(Roving Software License for a Hardware Agent)（案號：08/303,084)及"於一硬體媒介-基礎系統中提供一移動軟體許可之方法"(Method for Providing a Roving Software License in a Hardware Agent-Based System)（案號：08/472,951)。這些申請案由本發明相同之讓受者所擁有。

發明背景

1. 發明領域

本發明係相關於資料安全之領域。更特別的是，本發明揭示一種系統及方法，以防止機密資訊從一列印節點輸出，直到確認機密資訊之授權接收者接近列印節點。

2. 發明相關技藝敘述

由於接連的發展體積小、快速及更有效率的電腦，許多商業上目前實行"分送"(distributed)網路（如，區域網路等）。這些網路的優點是每個使用者可透過自己的個人電腦來控制。再者，由於經濟的考量，多使用者可連接較少使用的硬體元件，例如：位於可由所有使用者所存取之公用區域之列印節點。於本發明範圍中，一"列印節點"爲一獨立的硬體裝置，可接收、暫時地儲存及列印或顯示來自一個人電腦或其他傳送裝置之資料。例如，一列印節點可爲一

五、發明說明（2 ）

印表機，一結合一列印伺服器操作之印表機，一傳眞機器，一繪圖機(plotter)，一遠端監控器等等。

分送網路經常產生的問題包括保護文件中機密或專用的資訊(此後稱之爲"敏感的"文件)，被位授權的人錯誤地或蓄意地讀取。由於列印節點係位於公用區域，一經由列印節點傳送一列印工作，傳送者必須立即地趕到列印節點以取得敏感文件，以保護所包含之機密資訊。在此情況下，列印節點經驗一暫時的問題(如，擁塞、沒有紙張、碳粉不足等等)，或與其他列印工作佇列，傳送者必須於列印節點等待問題被更正或等待列印工作被執行。

另外，假如可以的話，傳送者可返回其電腦並取消有關於敏感文件之列印工作。但是，當然必須冒著當傳送者在返回電腦的期間，文件有可能被列印或顯示的風險。但是，假如列印工作錯誤地被傳送至不同的列印節點，可能爲一離站的(off-site)列印節點，則具有較少的選擇以保護敏感文件不被列印或顯示，且可能被一個未授權者所讀取，假如傳送錯誤在列印工作開始之後才被偵測。

不論分送網路中的列印工作可能或不可能被取消，使用者都浪費了寶貴的工作時間在等待列印節點之敏感文件上。如此之時間浪費不幸地影響的傳送者及其公司的生產力。

分送網路所經常產生的另一問題是保護敏感文件中的機密資訊在列印時不被另一工作站之其他的人公用觀看(如，合作的工作者)。當然，敏感文件可以加密的格式電子

五、發明說明（3 ）

式地寄給合作的工作者。然而有時候，由於改變及/或電子地傳送至未預定接收者，可能不經意地以電子式地傳送一敏感文件。當然，文件可被列印且郵寄至合作的工作者，然而時間延遲、郵寄安全等顯著的缺點必然會存在。因此，必須有效的建立一種系統及方法，以消除有關傳送者或其他預定接收者之保護列印節點列印敏感資訊之缺點。

發明概述

本發明揭示一種系統及方法，以防止一文件的拷貝從一列印節點輸出，直到列印節點辨識預定接收者。此系統包括一個傳送節點，一個列印節點及一個通訊鏈將這些節點以網路的方式連接。傳送節點存取列印節點的公用鍵，並於透過通訊鏈傳送至列印節點之前，利用此公用鍵加密一表頭及檔案。列印節點存取其專用鍵以解密表頭，以確定文件是否爲"敏感的"(即，在列印之前要求接收者授權)。假如如此，列印節點區域地緩衝暫存文件直到接收授權以輸出該文件。

圖式簡述

本發明的其他特點與優點將由詳細說明及伴隨之圖式加以突顯，如下：

圖1顯示一分送、安全網路系統之簡單的方塊圖，此網路系統包括一傳送節點及一列印節點。

圖2a及2b顯示一網路系統之方塊圖，此網路系統利用關於列印節點之公用鍵及傳送一加密表頭和從傳送節點至列印節點之文件的不同辨識方法。

五、發明說明（4）

圖3爲一流程圖，顯示一標示包含機密資訊之敏感文件在接收者確認之前將不會輸出。

發明詳細敘述

本發明係相關於一種裝置及方法，以防止列印節點之敏感文件的列印，直到預定接收者授權如此之列印發生。雖然利用詳盡的說明以達到對本發明通盤的了解，對於一般熟知此技藝者而言，可在不悖離發明精神與範圍之情況下，實行所述之實施例以外的不同實施例。另外，習知的電路、元件等並不加以說明，以避免與本發明造成不必要的混淆。

在詳細說明中，多個密碼通訊-相關(cryptography-related)的名詞通常用以敘述這裡所定義的特定特徵或性質。一個"鍵"(key)爲一習知密碼通訊演繹法知編碼及/或解碼參數。更特別的是，該鍵爲一循序的"n"位元長度之二進位資料之分配("字串")，其中"n"爲任意數。一個"文件"通常以預定之資料量來定義，例如：以一匯流排週期順序傳送之一或多頁資料。一"數位辨識"(digital certificate)爲一組數位資訊，由眾所皆知的企業授權(例如，銀行、政府機構、商業組織、元件製造商、公司保全、系統管理等等)透過一專用鍵的使用密碼通訊地結合在一起。一個"數位簽名"(digital signature)爲一相似的技術，以利用訊息發送者之專用鍵來確保訊息的完整性。

參考圖1，顯示一簡單的分送、保全網路系統，以防止敏感文件被錯誤地列印。保全網路系統100包括至少一傳

五、發明說明（5）

送節點110，透過通訊線120連接至一列印節點130。雖然未顯示，更多的傳送節點可透過類似線120之分享或獨立通訊，傳送至列印節點130。當保全網路系統獲得較大的商業容納，文件在置於商業鏈120之前，通常於傳送節點110中加密。此將防止機密資訊之無照增益存取，當其被傳送至列印節點130時。因此，列印節點130最好包括軟體或硬體，例如上述的相關參考申請案所揭示，以於輸出之前解密文件。

現在參考圖2a-2b，顯示利用傳送和列印節點110與130所採用的不對稱鍵技術之網路系統的實施例。此不對稱技術利用兩個不同的鍵(如一"公用鍵"及一"專用鍵")，以作爲加密及解密。爲了建立從傳送節點110至列印節點130的單一方向通訊，列印節點("PUK")之公用鍵應被初始化爲可透過多種辨識方法之一，例如透過一網路-基礎的印表機-鍵伺服器、當該等節點加入網路時，透過一具有相關印表機公用鍵之所有網路節點之初始化、或透過任一種可能的方法，來存取傳送節點110。這些可能的方法的每一個皆可利用一或多個由至少一委託的授權(trusted authorty)所發佈之數位辨識，以獲取PUK並實體化列印節點之授權。

圖2a中顯示一種獲取及確認PUK的方法。一委託的授權例如一列印節點製造商225製造列印節點130，該列印節點於列印節點130中所完成之非揮發性儲存元件205中具有一公用鍵("PUK")210及一專用鍵("PRK")211。此外，製造

五、發明說明（6）

商225於非揮發性儲存元件205中儲存一列印節點辨識("PNCert") 215。列印節點辨識PNCert 215至少相當於製造商225之專用鍵("PRKM") 226所加密的PUK 210。在傳送節點110之非揮發性儲存元件235之PUK的辨識及儲存之後，PNCert 215亦可儲存於非揮發性儲存元件235中。如此之儲存爲可選擇的，因爲PNCert 215將不再需要除非PUK 210毀壞或意外地從傳送節點110中移除。

在將列印節點連接一網路並將PNCert 215分送連接網路的傳送節點110之後，傳送節點110可利用PNCert 215以辨識(i)在初始分送之列印節點公用鍵("PUK")之授權(ii)列印節點之特性(即，是否可實行接受者授權程序)。如此之辨識可由區域委託的授權230(即，一系統管理員或一擁有列印節點實體之保全公司)，發佈一確認辨識("VCert") 240爲區域委託授權("PRKLTA") 231所加密之製造商("PUKM") 227之公用鍵來完成。區域委託授權("PRKLTA") 232之公用鍵將可廣泛地爲網路使用者所使用。確認辨識240可被解密以獲取PUKM 207，其可由解密PNCert 215來獲取PUK 210。

圖2b顯示可獲得確認PUK之另一方法的例子，其中區域委託的授權230在將其提供給傳送節點110之前，內部地辨識PUK。如所示，區域委託的授權230由利用列印節點製造商"PUKM" 227之公用鍵來解密PNCert 215，從列印節點130獲取PUK 210。其後，區域委託的授權230建立一區域產生的確認辨識("LVCert") 245並將LVCert 245傳送至傳

五、發明說明（7 ）

送節點110。與圖2a之PNCert相似的，假如需要的話在PUK 210辨識之後，LVCert 245可儲存於非揮發性記憶體元件235中。傳送節點110利用廣泛使用的PUKLTA 231來解碼LVCert 245。結果，傳送節點110獲取次順序於儲存非揮發性記憶體元件235中的PUK 210。

如圖2a與2b所示，在優先權節點130之公用鍵"PUK" 210可傳送至傳送節點110之後，傳送節點110可利用PUK 210之不對稱的"Rivest Shamir Adlemann" ("RSA")演繹法加密一文件250。此形成一加密的文件255以傳送至列印節點130。此外，文件之表頭260利用產生一加密表頭265之目標的列印節點130之公用鍵"PUK" 210來加密。替代列印工作之RSA加密，"表頭"可包括一之後由傳送者與接收者所用之"區段鍵"(session key)，以執行文件所需的密碼通訊操作。眾所皆知的是："表頭"爲減少一般相關公用鍵密碼通訊計算執行，特別是大資料組的一般技術。然而，對於本發明而言，表頭260包括允許列印節點130以支援不同功能之控制資訊。

例如，表頭260可包括控制資訊，假如機密程度超過一預定(或正常)的程度，其由選擇文件具有一特定的"機密"程度，藉此於列印之前要求預定接收者之上站(on-site)授權指示文件爲一敏感文件。另一例子爲關於表頭260包括一敏感文件之列印拷貝之預定接收者的公用鍵。因此，在列印"敏感"文件之前，列印節點130將透過利用預定接收者之公用鍵之一種授權技術(於下說明)確認該預定接收者

五、發明說明（8 ）

。另一例子爲控制資訊可包括標籤資訊，例如一"惟獨列印"(print only)標籤。此標籤將允許"敏感"文件250從列印節點130列印，但不允許文件250以文字格式儲存於記憶體中。此"惟獨列印"(print only)標籤之區域擴展爲控制資訊，包括一指示"敏感"文件可被列印次數之參數。

在一較佳實施例中，列印工作爲一連續的加密表頭265且加密的文件255透過一公用領域(public domain) 270轉換並進入列印節點130。列印節點130首先利用PRK 211解密加密的表頭265，以確定加密的文件255是否包括機密資訊，其要求列印節點130以至少避免列印該文件250，直到預定的接收者在列印節點130出現。因此該文件250最好暫時地儲存於列印節點130中的緩衝記憶體(未顯示)，但是不需要以加密的格式儲存。一旦接收確認預定的接收者出現時，加密文件250(i)從緩衝記憶體擷取，(ii)被解密，及(iii)被列印。

當文件未被擷取或緩衝記憶體變成滿的時，預期可能存在一些情況。在這些及相關的情況下，從緩衝記憶體"更新"(即從記憶體刪除)特定未擷取的文件，藉此釋放記憶體空間是必須的。此可自動地透過軟體及/或硬體或手動地由系統管理員，網路使用者等等來執行。

有一些授權技術來確認預定接收者存在於列印節點。其中一個技術是等待一透過鍵盤輸入之預定接收者之個人的辨識號碼("PIN")，及開始一敏感文件之列印工作之前列印節點上的數字板(number pad)。在此情況下，列印節點可

五、發明說明（9 ）

包括相關每個辨識公用鍵之記憶體儲存PINs，或PIN可透過表頭傳送至列印節點。

另一技術爲透過鍵盤輸入"釋放碼"(release code)。釋放碼爲列印時間由傳送節點所產生的特定-工作並包含於表頭中。釋放碼係於短時間週期顯示於電腦的顯示螢幕上，以提供使用者足夠的資訊以擷取列印工作。假如預定接受者不是傳送的使用者，傳送的使用者可透過一電話呼叫、電子郵件、或其他裝置與預定接收者通訊釋放碼。

再另一個技術爲利用授權的表徵字(token)，例如PCMCIA辨識元卡或可插入列印節點之智慧卡。取代要求列印節點以維護表徵字辨識之記錄，表徵字的公用鍵可包含於表頭中，並且最好以加密的格式傳送至列印節點。因此，列印節點需要簡化表徵字的公用鍵與之前在列印工作標頭所接收公用鍵的匹配，並以表徵字執行一標準的詢問/回應(challenge/response)協定。如此的challenge/response協定確認該表徵字由提供具有相應特定-表頭公用鍵專用鍵之表徵字來授權。

第四個技術爲利用一稱爲"生物測定學"(biometrics)的存取控制技術，該技術起初利用一保全設施(即建築物、房間等等)之獲取裝置。生物測定學包括感測一使用者的特性(即，指紋、虹彩、視網膜等等)，以獲取一單一的資料框(通常稱爲"資料框")，或多個特性的資料框，並將獲取的資料框與前所儲存的主體(master)相比較。假如每個所獲取的資料框與儲存的主體正確地比較，使用者被辨識並

五、發明說明（10）

被授權。

現在參考圖3，顯示一網路系統操作的流程圖。首先，該文件必須被辨識爲"敏感"文件，一取決於機密及/或專有資訊是否包含於文件之一般文件(步驟300)。假如爲一般文件，一旦將文件傳送至一列印節點，傳送節點建立一表頭，該表頭包括揭示保護資訊，例如限制文件只被列印之、減輕修改文件任何機會的"惟獨列印"標籤(步驟305-310)。其後，表頭及文件在被傳送給列印節點之前加密。

然而，假如文件不是"敏感"文件，一旦將文件傳送給一列印節點，傳送節點建立一表頭，該表頭包括必須授權預定接收者之資訊(公用鍵、表徵字等等)，及額外揭示保護所需的任何資訊(步驟305，315)。假如授權資訊爲一釋放碼，釋放碼必須於傳送節點之顯示螢幕上顯示，以致能預定接收者指示列印節點開始列印敏感文件(步驟320及325)。其後，表頭及文件被加密形成一列印工作且此列印工作被傳送致列印節點(步驟330)。

一旦接收此列印工作，列印節點解密表頭以決定文件是否爲一"敏感文件"(步驟335及340)。假如文件爲一般的文件，列印節點解密該文件(步驟355)，並接著列印該文件(步驟360)。但是，假如爲一敏感文件，列印節點儲存加密的文件於一內部的緩衝記憶體中(步驟345)，並等待鄰近列印節點之預定接收者的授權(步驟350)。一旦透過提供一PIN、釋放碼、一授權表徵字等接收授權，該列印節點解密文件且其後列印該文件(步驟355及360)。預期敏感文

五、發明說明（11）

件可於步驟345之前解密，所以預定接收者一被辨識，敏感文件被列佇列印並被列印(步驟360)。

在前所述之說明中，本發明已由許多不同的方法並利用許多不同的建構加以說明。然而，在不悖離本發明之精神及範圍之情況下亦可做不同的修正及改變。本發明所提出的申請專利範圍如下所述。

四、中文發明摘要（發明之名稱：經由在列印節點上之使用者辨識以防止揭露之裝置）及方法

本發明揭示一種系統及方法，以防止一文件的拷貝從一列印節點輸出，直到列印節點辨識預定接收者。此系統包括一個傳送節點，一個列印節點及一個通訊鏈將這些節點以網路的方式連接。傳送節點存取列印節點的公用鍵(public key)，並於透過通訊鏈傳送至列印節點之前，利用此公用鍵加密(encrypt)一表頭(header)及檔案。列印節點存取其專用鍵(private key)以解密(decrypt)表頭，以確定文件是否在輸出之前由預定接收者要求辨識。

英文發明摘要（發明之名稱：APPARATUS AND METHOD FOR PREVENTING DISCLOSURE THROUGH USER-AUTHENTICATION AT A PRINTING NODE）

A system and method for preventing a copy of a document to the output from a printing node until the printing node authenticates the intended recipient. The system includes a sending node, a printing node and a communication link coupling these nodes together in a network fashion. The sending node has access to a public key of the printing node and uses this public key to encrypt,a header and document before transmission to the printing node over the communication link. The priority node has access to its private key to decrypt the header to ascertain whether the document requires authentication by the intended recipient before being output.

六、申請專利範圍

1. 一種方法，其防止一列印節點輸出一文件的拷貝，直到一文件的預定接收者被授權接近列印節點，該方法包括下面步驟：

選定一文件之機密程度，其中文件爲列印工作的一部份：

建立一列印工作之表頭，假如該機密程度大於或等於一預定程度的話，該表頭爲一第一表頭，該第一表頭包括至少(i)資訊以授權該接受者及(ii)至少包括該機密程度之控制資訊；

將該列印工作傳送至列印節點：

分析該表頭以判定機密程度是否大於或等於該預定程度，其中假如是的話，一旦接收者被授權則輸出該文件。

2. 根據申請專利範圍第1項之方法，其中該表頭由該列印工作中建立一表頭的步驟所建立，假如該機密程度被選定爲小於該預定程度的話，包括一第二表頭，該第二表頭包括控制資訊。
3. 根據申請專利範圍第2項之方法，其中在該傳送步驟之前，該方法尚包括以一列印節點公用鍵加密該表頭的步驟。
4. 根據申請專利範圍第3項之方法，其中在該傳送步驟之前，該方法尚包括以一列印節點公用鍵加密該文件的步驟。
5. 根據申請專利範圍第3項之方法，其中在該傳送步驟之

六、申請專利範圍

後，該方法尚包括以一列印節點專用鍵解密該表頭，以判定該機密程度的步驟。

6. 根據申請專利範圍第4項之方法，其中在分析該表頭之後及在該輸出文件一經接收者授權之前，該方法尚包括下面步驟：

由該列印節點公用鍵以一加密格式緩衝該文件；及

一經接收者授權後以一列印節點的專用鍵解密該文件。

7. 一種方法，其防止一列印節點輸出一文件的拷貝，直到一文件的預定接收者被授權接近列印節點，該方法包括下面步驟：

建立一該列印工作之第一表頭，該第一表頭包括至少(i)資訊以授權該接受者及(ii)至少包括該機密程度之控制資訊；

以列印模態之公用鍵加密該第一表頭及該列印工作之文件；

將該列印工作傳送至列印節點；

將加密的文件儲存於列印節點中；及

一旦接收者被授權之後，解密加密的文件並列佇輸出的文件。

8. 根據申請專利範圍第7項之方法，其中該表頭的控制資訊包括一接收者的公用鍵。

9. 根據申請專利範圍第1項的方法，其中該控制資訊包括一惟獨-列印標籤。

六、申請專利範圍

10. 一種方法，其防止一列印節點輸出一文件的拷貝，直到一文件的預定接收者被授權接近列印節點，該方法包括下面步驟：

選定一文件之機密程度，其中文件爲列印工作的一部份：

建立一列印工作之表頭，其中

假如該機密程度大於或等於一預定程度的話，該表頭爲一第一表頭，該第一表頭包括至少(i)資訊以授權該接受者及(ii)至少包括該機密程度之第一控制資訊組：

假如該機密程度小於該預定程度，該表頭爲一包括一第二控制資訊組之第二表頭：

加密該列印工作；

將該列印工作傳送至列印節點；

解密該表頭以獲取機密程度，其中

假如該機密程度大於或等於該預定程度，

暫時地儲存該文件，及

一旦接收者被授權則輸出該文件；

假如機密程度小於該預定程度，

預備將由列印節點輸出的文件。

11. 一種系統建構，其防止一文件的拷貝從一列印節點輸出，直到列印節點從一預定接收者接收區域的授權，該系統包括：

一通訊鏈：

六、申請專利範圍

一連接該通訊鏈之傳送節點，該傳送節點包括一儲存元件，該儲存元件包含至少一相關該列印節點之公用鍵，該傳送節點在傳送至列印節點之前，經由該通訊鏈利用該公用鍵來加密一表頭及文件；及

連接該通訊鏈之列印節點，列印節點包括一儲存元件，該儲存元件包括至少一相關該列印節點之專用鍵，假如機密程度超過一預定程度，列印節點解密該表頭以獲取一文件的機密程度，並防止文件輸出直到在列印節點的接收者授權。

12. 根據申請專利範圍第11項的系統，其中該傳送節點爲一電腦。

13. 根據申請專利範圍第11項的系統，其中該列印節點爲包含印表機、繪圖機、傳眞機器及顯示螢幕組群中的一個。

14. 根據申請專利範圍第11項的系統，其中該傳送節點的儲存元件及該列印節點的儲存元件皆爲非揮發性記憶體。

15. 根據申請專利範圍第11項的系統，其中該列印節點的儲存元件尚包括一數位辨識，其至少爲以一委託授權之專用鍵加密的列印節點之公用鍵。

16. 根據申請專利範圍第11項的系統，其中該列印節點包括內部記憶體，用以直到接受者在列印節點被授權時儲存該文件。

17. 一種系統建構以立即地列佇從列印裝置輸出的非機密文

六、申請專利範圍

件，或防止一文件的拷貝從一列印節點輸出，直到列印裝置從一文件的預定接收者接收授權，即該預定接收者接近列印節點，該系統包括：

傳送裝置，用以加密具有一第一表頭的列印工作和具有一列印節點之公用鍵的機密文件，並用以將加密的第一表頭和加密的機密文件傳送至列印裝置，該傳送裝置包括一包含至少該公用鍵的第一儲存裝置；

列印裝置，用以解密該第一表頭、分析該第一表頭以判定該列印工作包含加密的機密文件，及防止機密文件被列印，直到在列印裝置的接受者授權；及

於該傳送裝置與該列印裝置之間通訊的裝置。

18. 根據申請專利範圍第17項的系統，其中該傳送裝置尚加密另一具有一第二表頭和具有該列印節點之公用鍵的非機密文件的列印工作，並將加密的第二表頭和加密的非機密文件傳送至該列印裝置。

19. 根據申請專利範圍第18項的系統，其中該列印裝置尚解密該第二表頭，藉此判定該另一列印工作具有非機密文件，並預備不具有接收者授權之被輸出的非機密文件。

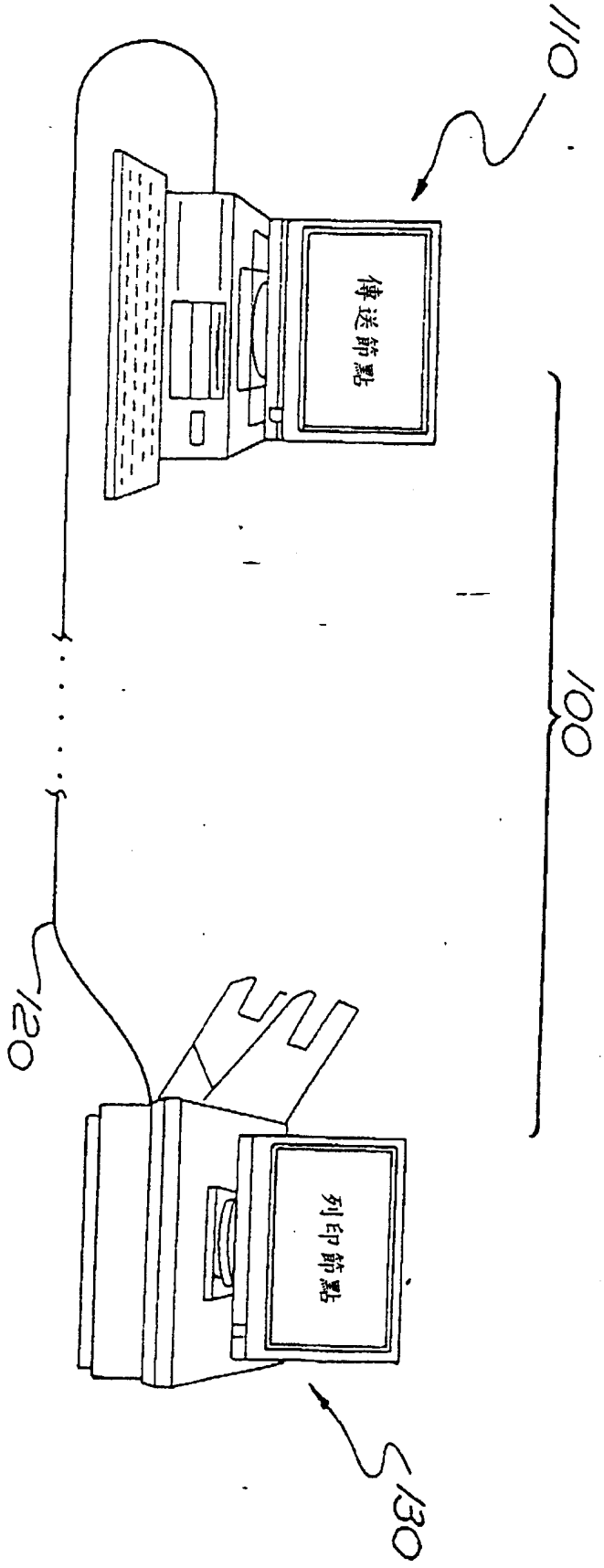

圖 1

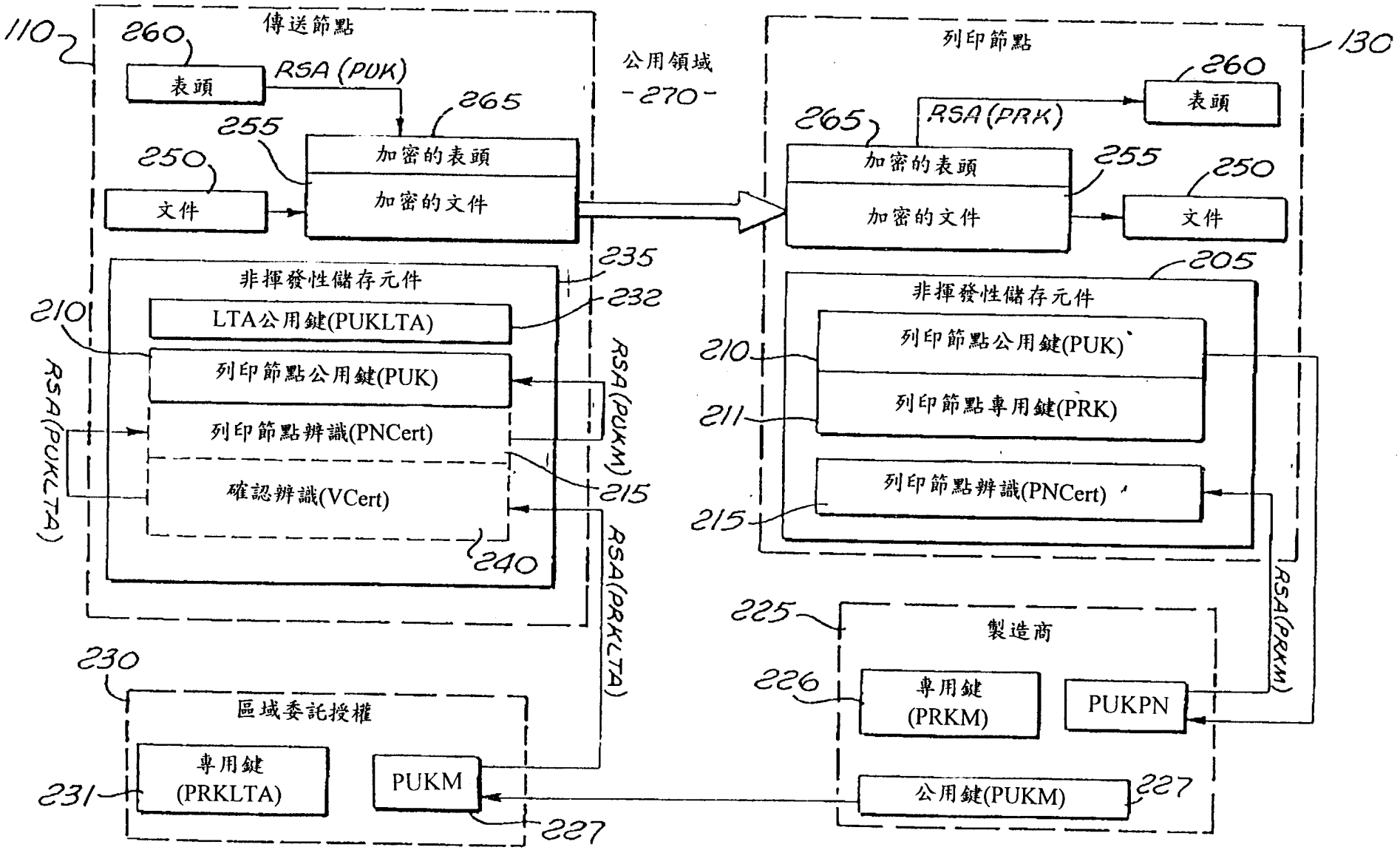
110
傳送節點
260
表頭
RSA (PUK)
265
255
加密的表頭
250
文件
加密的文件
非揮發性儲存元件
235
232
LTA公用鍵(PUKLTA)
210
列印節點公用鍵(PUK)
RSA(PUKLTA)
RSA(PUKM)
列印節點辨識(PNCert)
215
確認辨識(VCert)
240
RSA(PRKLTA)
230
區域委託授權
專用鍵
(PRKLTA)
231
PUKM
227
公用領域
-270-
列印節點
130
260
表頭
265
RSA(PRK)
加密的表頭
255
250
加密的文件
文件
205
非揮發性儲存元件
210
列印節點公用鍵(PUK)
211
列印節點專用鍵(PRK)
列印節點辨識(PNCert)
215
RSA(PRKM)
225
製造商
226
專用鍵
(PRKM)
PUKPN
公用鍵(PUKM)
227

圖 2a

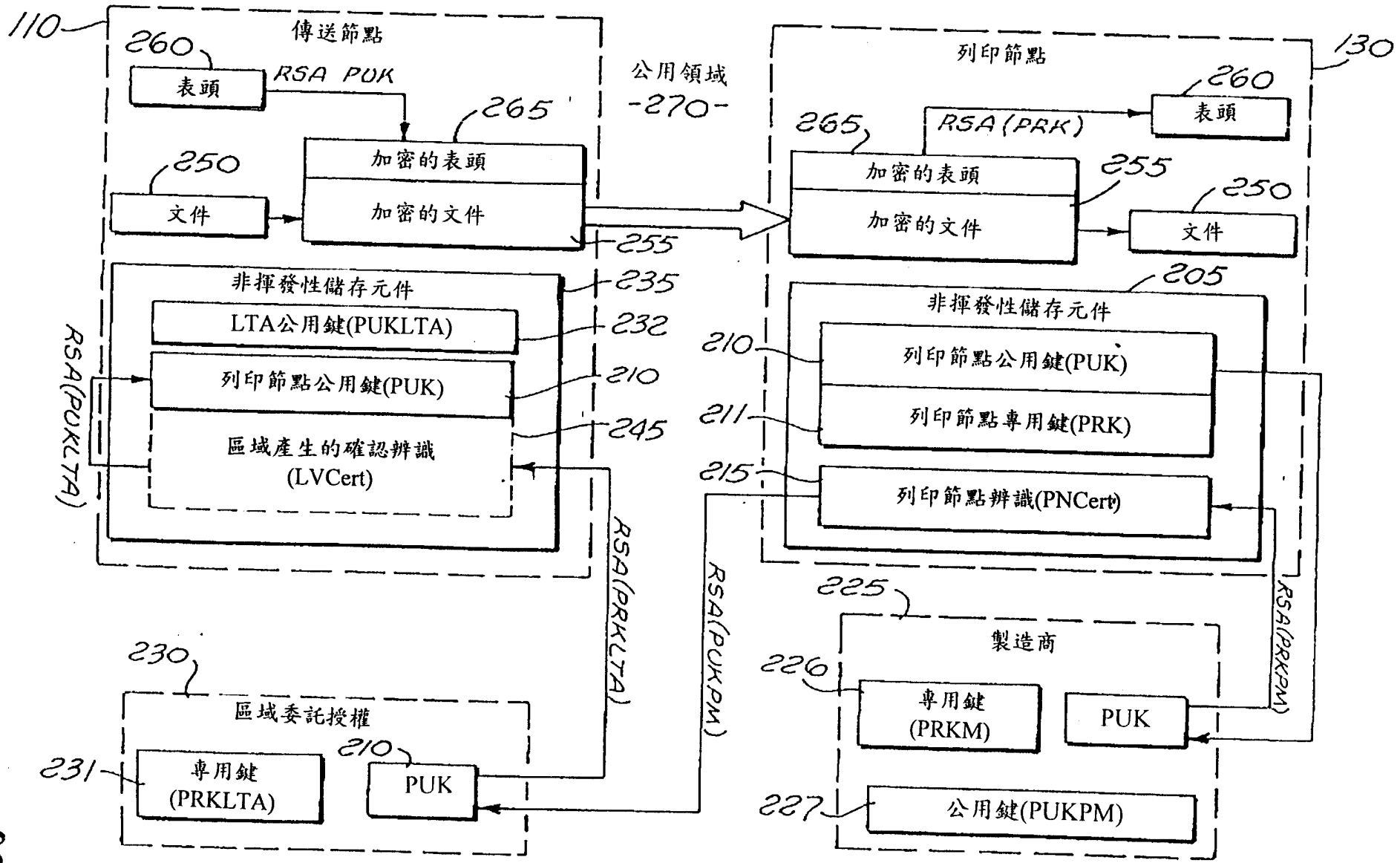
110
傳送節點
260
表頭
RSA PUK
265
加密的表頭
250
文件
加密的文件
255
公用領域
-270-
非揮發性儲存元件
235
LTA公用鍵(PUKLTA)
232
列印節點公用鍵(PUK)
210
區域產生的確認辨識
(LVCert)
245
RSA(PUKLTA)
RSA(PRKLTA)
230
區域委託授權
231
專用鍵
(PRKLTA)
210
PUK
RSA(PUKPM)
130
列印節點
260
表頭
265
RSA(PRK)
加密的表頭
255
加密的文件
250
文件
205
非揮發性儲存元件
210
列印節點公用鍵(PUK)
211
列印節點專用鍵(PRK)
215
列印節點辨識(PNCert)
RSA(PRKPM)
225
製造商
226
專用鍵
(PRKM)
PUK
227
公用鍵(PUKPM)

圖 2b

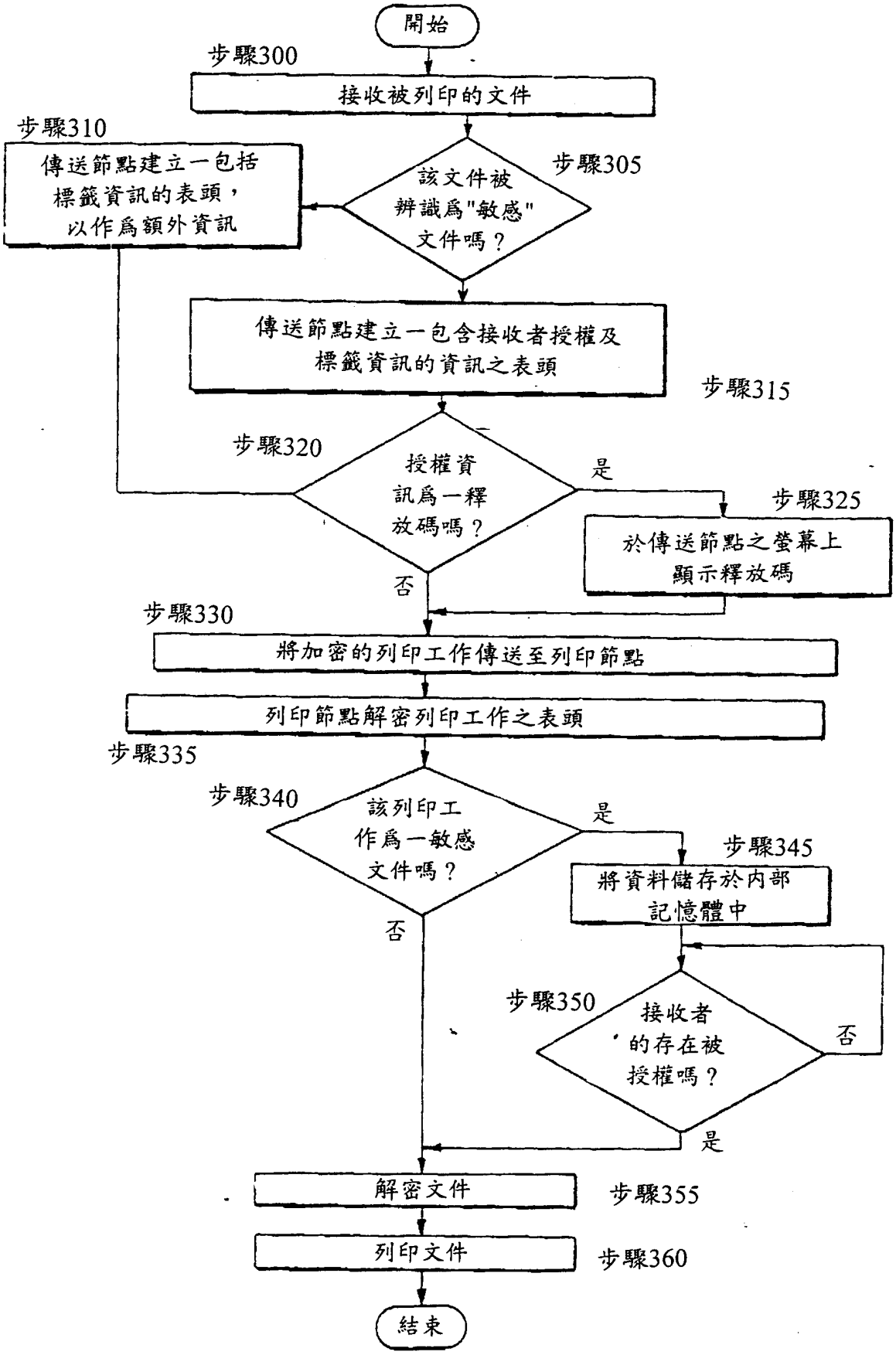
開始
步驟300
接收被列印的文件
步驟310
傳送節點建立一包括標籤資訊的表頭，以作爲額外資訊
該文件被辨識爲"敏感"文件嗎？
步驟305
傳送節點建立一包含接收者授權及標籤資訊的資訊之表頭
步驟315
步驟320
授權資訊爲一釋放碼嗎？
是
步驟325
於傳送節點之螢幕上顯示釋放碼
否
步驟330
將加密的列印工作傳送至列印節點
列印節點解密列印工作之表頭
步驟335
步驟340
該列印工作爲一敏感文件嗎？
是
步驟345
將資料儲存於內部記憶體中
否
步驟350
接收者的存在被授權嗎？
否
是
解密文件
步驟355
列印文件
步驟360
結束

圖 3