智慧財產及商業法院民事判決

113年度民專訴字第63號

原　　告　台灣善騰科技股份有限公司
法定代理人　李秋絨
訴訟代理人　尤彰澤律師
被　　告　連加網路商業股份有限公司
法定代理人　丁雄注
訴訟代理人　呂光律師
　　吳詩儀律師
　　吳弈錡專利師

上列當事人間侵害專利權有關財產權爭議等事件，本院於民國114年6月13日言詞辯論終結，判決如下：

主　文

原告之訴及假執行之聲請均駁回。

訴訟費用由原告負擔。

事實及理由

一、原告主張略以：

㈠原告為我國第I566564號「虛實身分驗證電路、系統及電子消費方法」發明專利（下稱系爭專利）之專屬被授權人，授權期間為民國109年7月23日至121年4月24日。原告於市場發現被告之「『line pay』行動支付具有以生物特徵(指紋、臉部等)進行該使用者的身分電子驗證之功能」（下稱系爭產品），提供予消費者於使用「line pay」付款時驗證其身分，而上開技術有落入系爭專利範圍之可能，遂將前揭「line pay」行動支付之產品說明等相關資訊，委請民間公證人做成網頁公證書，並將上開公證書及相關資料交付鑑定，鑑定結果認系爭產品落入系爭專利請求項1虛實身分驗證電路之專利權範圍，侵害系爭專利請求項1至8。

㈡原告遂於113年8月9日寄發律師函予被告，請求被告停止該侵權行為，並出面協商損害賠償或授權事宜未果。為此依專利法第96條第1項、第3項規定請求防止、排除被告侵害系爭

專利，並將流通至市面上之系爭產品予以刪除，另依同法第96條第2項、第97條第1項規定請求被告賠償損害。

㈢並聲明：

1.被告應給付原告新臺幣1,000萬元，及自起訴狀送達之翌日起至清償日止按年息百分之5計算之利息。

2.被告不得自行或使第三人直接或間接於「line pay」行動支付以生物特徵(指紋、臉部等)進行該使用者的身分電子驗證之功能，及停止提供上開功能予第三人使用，亦不得為其他一切侵害原告之系爭專利行為，且被告已流通至市面之上開「line pay」行動支付，其中以生物特徵(指紋、臉部等)進行該使用者的身分電子驗證之功能，應全部予以刪除。

3.願供擔保請准宣告假執行。

二、被告答辯略以：

㈠原告主張系爭產品侵害系爭專利請求項1，而原證8之鑑定報告書之鑑定範圍包括請求項1至8，則原告主張之請求項範圍為何，亦須先予特定。系爭產品不具有系爭專利請求項1至8物品專利之物之特徵，無構成侵權之可能。又原告提出之鑑定報告並非以系爭產品對應之技術內容進行侵權比對，原告未盡舉證之責。又原告主張被告於我國使用系爭產品，然原告提供比對資料中，原證8附件三之附件3為自國外（日本）網站下載之資料，並無與我國LINE Pay行動支付相關之說明，被告提供之LINE Pay行動支付服務，並未如原告所稱係依據國際Fast IDentity Online標準（下稱FIDO標準）提供客戶身分識別服務。

㈡原告援引「金融機構辦理快速身分識別機制安全控管作業指引」（下稱系爭作業指引），聲稱系爭產品必然符合FIDO標準之安全規定云云，然被告係屬提供「第三方支付」之服務業，受數位發展部監管，而非屬受金融監督管理委員會監管（下稱金管會）之「金融機構」，自未受到金管會相關法令之拘束。系爭作業指引僅為金管會之行政指導，並不具有法

律之拘束力，故原告以此文件指稱被告之LINE Pay行動支付服務必然符合FIDO標準云云，並無理由，是原告錯誤比對FIDO標準之文件，顯見鑑定結果與本件爭議無關。

㈢並聲明：原告之訴及其假執行之聲請均駁回；如受不利之判決，被告願以現金或等值之兆豐國際商業銀行可轉讓定期存單供擔保，請准宣告免為假執行。

三、兩造不爭執事項（見本院卷二第382至383頁）

㈠系爭專利經薩摩亞商善騰國際開發科技股份有限公司於101年4月25日向經濟部智慧財產局（下稱智慧局）申請取得發明專利，於106年1月11日經智慧局核准公告（原證1、2）。原告於109年7月23日取得系爭專利之專屬授權，授權期間至121年4月24日（原證6、7）。

㈡原告於113年8月9日委請律師寄發律師函予被告公司（原證9），請被告停止將系爭產品與消費者使用，並請被告出面協商損害賠償或授權事宜。

四、兩造所爭執之處，經協議簡化如下（見本院卷二第383頁）：

㈠專利侵權部分：

系爭產品是否落入系爭專利請求項1至8之文義範圍或均等範圍？

㈡專利有效性部分：

1.乙證2可否證明系爭專利請求項1至8不具新穎性？

2.乙證2可否證明系爭專利請求項1至8不具進步性？

3.乙證2、3之組合可否證明系爭專利請求項1至8不具進步性？

4.乙證2、4之組合可否證明系爭專利請求項1至8不具進步性？

㈢原告依專利法第96條第1項、第3項規定，請求被告防止、排除侵害系爭專利，及將流通至市面上之系爭產品予以刪除有無理由？

㈣被告有無侵害系爭專利之故意或過失？原告依專利法第96條第2項、第97條第1項規定，請求被告給付損害賠償有無理由？若有，金額為何？

五、系爭產品未落入系爭專利請求項1至8之文義或均等範圍

㈠系爭專利技術分析

1.技術內容

系爭專利發明之虛實身分驗證電路、系統及電子消費方法，係可提供使用者藉由該虛實身分驗證電路將本身的生物特徵，經由複數種處理程序之至少其一者的演算而形成基於該生物特徵的該生物特徵碼，而該生物特徵碼係可透過遠端的認證伺服主機進行該使用者的身分電子驗證，而該認證伺服主機係可驗證該生物特徵碼是否符合在該認證伺服主機所存放與該使用者相關的該生物特徵，進一步將驗證的結果係回傳至該虛實身分驗證電路，用以完成該使用者的身分電子驗證（見系爭專利發明說明書，本院卷一第38頁）。

2.系爭專利之虛實身分驗證電路的方塊示意圖如附圖1所示（見本院卷一第47頁）。

3.系爭專利申請專利範圍（見本院卷一第41至46頁）

系爭專利請求項共計18項，其中請求項1、9、12為獨立項，其餘為附屬項。原告主張受侵害者為系爭專利請求項1至8，其內容如下：

請求項1：一種虛實身分驗證電路，係供內建於電子裝置或與該電子裝置連接，用以讓使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證，其中該認證伺服主機係儲存與該生物特徵相關的訊息，該虛實身分驗證電路係包含：記憶單元，係具有儲存空間，該儲存空間儲存驗證金鑰碼；擷取單元，係供擷取該生物特徵，該擷取單元係根據擷取的該生物特徵產生相對應的生物特徵碼，其中該擷取單元可透過指紋辨識器或攝影機擷取

該生物特徵；處理單元，係連接該記憶單元與該擷取單元，該處理單元係具有處理程序，且該處理單元係基於該處理程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼，其中該待驗證碼具有該生物特徵碼與該驗證金鑰碼之至少一者；以及通訊單元，係與該處理單元連接，該通訊單元將該待驗證碼傳送至該網際網路，以及等待該認證伺服主機回傳與該待驗證碼相關該身分電子驗證的驗證結果；其中該通訊單元係接收動態金鑰碼並將該動態金鑰碼儲存至該記憶單元而在該記憶單元形成該驗證金鑰碼，且該動態金鑰碼是被動式更換或主動式更換。

請求項2：如申請專利範圍第1項所述的虛實身分驗證電路，其中該記憶單元係為預先地儲存與該生物特徵相關的本地驗證金鑰。

請求項3：如申請專利範圍第2項所述的虛實身分驗證電路，其中該處理單元係在基於該處理程序比對該生物特徵碼與該驗證金鑰碼，用以決定是否產生該待驗證碼。

請求項4：如申請專利範圍第1項所述的虛實身分驗證電路，其中該記憶單元係為儲存與該電子裝置相關的該驗證金鑰碼，用於供該處理單元基於該處理程序編碼該生物特徵碼與該驗證金鑰碼以產生相對應於該生物特徵碼與該驗證金鑰碼的該待驗證碼。

請求項5：如申請專利範圍第4項所述的虛實身分驗證電路，其中該驗證金鑰碼係為來自於該電子裝置的媒體存取控制位址(Media Access Control Address)、用戶身份模塊(Subscriber Identity Module)與用戶自訂密碼之至少其一者。

請求項6：如申請專利範圍第1項所述的虛實身分驗證電路，其中該生物特徵係指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者。

請求項7：如申請專利範圍第1項所述的虛實身分驗證電路，其中該通訊單元係以有線通訊型態或是無線通訊型態傳送該待驗證碼。

請求項8：如申請專利範圍第1項所述的虛實身分驗證電路，其中該通訊單元係符合藍芽(Bluetooth)、固網通訊、行動通訊、無線保真(Wi-Fi)的通訊協定。

㈡系爭產品技術內容

1.系爭產品之技術描述

依原告所提專利侵害鑑定報告（見原證8，本院卷一第101至143頁）可知，原告所指侵權產品為LINE Pay行動支付產品，其可供使用者安裝於其行動裝置並於啟動行動支付功能後，能與遠端認證伺服主機進行使用者的身分電子驗證之功能。

2.系爭產品相關操作之截圖如附圖2所示。

㈢系爭產品未落入系爭專利請求項1至8之文義範圍或均等範圍

1.系爭專利請求項1，其技術內容可拆解為6個要件：

⑴要件編號1A：「一種虛實身分驗證電路，係供內建於電子裝置或與該電子裝置連接，用以讓使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證，其中該認證伺服主機係儲存與該生物特徵相關的訊息，該虛實身分驗證電路係包含：」；

⑵要件編號1B：「記憶單元，係具有儲存空間，該儲存空間儲存驗證金鑰碼；」；

⑶要件編號1C：「擷取單元，係供擷取該生物特徵，該擷取單元係根據擷取的該生物特徵產生相對應的生物特徵碼，其中該擷取單元可透過指紋辨識器或攝影機擷取該生物特徵；」；

⑷要件編號1D：「處理單元，係連接該記憶單元與該擷取單元，該處理單元係具有處理程序，且該處理單元係基於該處理程序編碼該驗證金鑰碼與該生物特徵碼而產生

相對應的待驗證碼，其中該待驗證碼具有該生物特徵碼與該驗證金鑰碼之至少一者；以及」；

⑸要件編號1E：「通訊單元，係與該處理單元連接，該通訊單元將該待驗證碼傳送至該網際網路，以及等待該認證伺服主機回傳與該待驗證碼相關該身分電子驗證的驗證結果；」；

⑹要件編號1F：「其中該通訊單元係接收動態金鑰碼並將該動態金鑰碼儲存至該記憶單元而在該記憶單元形成該驗證金鑰碼，且該動態金鑰碼是被動式更換或主動式更換。」。

2.系爭產品技術內容與系爭專利請求項1比對

⑴要件編號1a

依原告提出之網頁資料（見原證10之附件2，本院卷二第55至71頁）可知，系爭產品可供使用者安裝於其行動裝置並於啟動行動支付功能後，能與遠端認證伺服主機進行使用者的身分電子驗證之功能，其中所述之「行動裝置」可對應系爭專利請求項1之「一種虛實身分驗證電路，係供內建於電子裝置或與該電子裝置連接」。另依原告所稱系爭產品係使用FIDO標準進行使用者身分之驗證和交易之確認（見本院卷二第47頁），而依原告提出之鑑定報告（見原證8之附件三、附件四，本院卷一第193至241頁)可知，系爭產品基於FIDO標準於使用者在註冊階段會產生公鑰和私鑰對，私鑰綁定生物辨識於使用者行動裝置，公鑰與使用者身分資訊一起註冊在FIDO伺服器，於驗證階段時，使用者可透過該行動裝置完成生物特徵辨識解鎖私鑰並以此私鑰對該伺服器提供之亂數(Challenge)進行亂數運算，並將亂數運算之結果傳回到該伺服器，該伺服器將該亂數運算之結果與其對應的公鑰進行驗證並回傳驗證結果，其中所述之「伺服器」雖可與使用者進行該使用者的身分電子驗證，惟該伺服器並未儲存使用者生物特徵相關的訊息，即系爭產

品並未具有可對應系爭專利請求項1「用以讓使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證，其中該認證伺服主機係儲存與該生物特徵相關的訊息」之技術內容。據此，系爭產品未為系爭專利請求項1要件編號1A所文義讀取。

⑵系爭產品要件編號1b、1f

系爭產品於驗證階段時，使用者可透過行動裝置完成生物特徵辨識解鎖私鑰，並以此私鑰對FIDO伺服器提供之亂數進行亂數運算，已如前述，是該行動裝置當具有可對應系爭專利請求項1之「通訊單元」及「記憶單元」，以接收並儲存FIDO伺服器提供之亂數，又所述之「亂數」可對應系爭專利請求項1之「動態金鑰碼」及「驗證金鑰碼」。據此，系爭產品因可供使用者安裝於行動裝置，致使其可為系爭專利請求項1要件編號1B、1F所文義讀取。

⑶要件編號1c

系爭產品於驗證階段時，使用者可透過行動裝置完成生物特徵辨識解鎖私鑰，已如前述，是該行動裝置當具有可對應系爭專利請求項1之「擷取單元」，以擷取使用者生物特徵並產生相對應的生物特徵碼以解鎖私鑰。據此，系爭產品因可供使用者安裝於行動裝置，致使其可為系爭專利請求項1要件編號1C所文義讀取。

⑷要件編號1d

系爭產品於驗證階段時，使用者可透過行動裝置完成生物特徵辨識解鎖私鑰並以此私鑰對伺服器提供之亂數進行亂數運算，並將亂數運算之結果傳回到伺服器，已如前述，是該行動裝置當具有處理單元，以將私鑰與亂數進行亂數運算，其中所述之「亂數運算之結果」雖具有可對應系爭專利請求項1驗證金鑰碼之亂數，惟系爭產品並未具有可對應系爭專利請求項1所述「基於該處理

程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼」之技術內容，即所述之「亂數運算之結果」不同於系爭專利請求項1之「待驗證碼」。據此，系爭產品未為系爭專利請求項1要件編號1D所文義讀取。

⑸要件編號1e

系爭產品於驗證階段時，使用者可透過行動裝置完成生物特徵辨識解鎖私鑰並以此私鑰對伺服器提供之亂數進行亂數運算，並將亂數運算之結果傳回到伺服器，伺服器將該亂數運算之結果與其對應的公鑰進行驗證並回傳驗證結果，而該行動裝置具有通訊單元，已如前述，惟系爭產品所述之「亂數運算之結果」不同於系爭專利請求項1之「待驗證碼」，亦如前述，即系爭產品並未具有可對應系爭專利請求項1所述「將該待驗證碼傳送至該網際網路，以及等待該認證伺服主機回傳與該待驗證碼相關該身分電子驗證的驗證結果」之技術內容。據此，系爭產品未為系爭專利請求項1要件編號1E所文義讀取。

3.原告稱：系爭產品受電子支付機構資訊系統標準及安全控管作業基準、金融機構運用新興科技作業規範、金融機構提供行動裝置應用程式作業規範及金融機構辦理電子銀行業務安全控管作業規範等相關規定，可證明系爭產品侵害系爭專利云云（見言詞辯論筆錄原告庭提附件，本院卷二第391頁）。然查：

⑴該附件記載：「電子支付機構資訊系統標準及安全控管作業基準一項第四款第三目規定：……電子支付機構應直接或間接驗證該生物特徵。1、採用直接驗證生物特徵技術者，電子支付機構應確認真人(Liveness Detection)、本人(Biorecognition)辦理並符合「金融機構運用新興科技作業規範」有關生物特徵資料安全控管部分……2、採用間接驗證生物特徵技術者，電子支付機構應事先評估使用者端設備驗證機制之有效性，善盡告知

使用者使用上之風險，並提供間接驗證機制關閉管道，必要時應加強防護機制……」、「依金融機構運用新興科技作業規範第五條第一項第九款規定：應於首次使用生物辨識技術、每年定期或技術有重大變更時(如輔助資料、技術提供商)，由資訊單位檢視該技術應足以有效識別客戶身分……」，即電子支付機構驗證使用者之生物特徵包含直接或間接驗證方式，原告並未能證明系爭產品之驗證方式係對應該基準之直接抑或間接方式?遑論證明該等作業基準或規範可使系爭產品具有可對應系爭專利請求項1要件編號1A「用以讓使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證，其中該認證伺服主機係儲存與該生物特徵相關的訊息」之技術內容。

⑵依該附件記載：「依金融機構運用新興科技作業規範第五條第一項……(二)假名標識符：是指用於生物特徵比對之資料，其內容不為原始生物特徵資料之一部份。(三)輔助資料：是指一演算法或機制，用來將原始生物特徵資料分離產生假名標識符……」、「電子支付機構資訊系統標準及安全控管作業基準第五條第一項第二款：網際網路或行動網路：應符合訊息隱密性、訊息完整性、訊息來源辨識性及訊息不可重複性之訊息防護措施....」、「電子支付機構資訊系統標準及安全控管作業基準第六條……二、訊息完整性：應採用……加密運算……四、訊息不可重複性：應採用序號、一次性亂數、時間戳記等機制產生……」、「金融機構辦理電子銀行業務安全控管作業基準訊息保護第四條……三、金鑰交換機制：採對稱性加解密時，其金鑰交換可分訊息加密金鑰與金鑰保護金鑰之交換……」、「金融機構辦理電子銀行業務安全控管作業基準訊息保護第五條……一、訊息傳輸……二、訊息儲存……(二)身分核驗資訊之生物特徵……」之內容，並未見具有對應系爭專利請

求項1要件編號1D所述「基於該處理程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼」、要件編號1E所述「將該待驗證碼傳送至該網際網路，以及等待該認證伺服主機回傳與該待驗證碼相關該身分電子驗證的驗證結果」之內容，尚難證明該等作業基準或規範可使系爭產品具有可對應系爭專利請求項1該要件編號1D、1E之技術內容。

4.綜上，系爭產品未為系爭專利請求項1之要件編號1A、1D、1E所文義讀取，故系爭產品未落入系爭專利請求項1之文義範圍。

5.系爭產品與系爭專利請求項1之均等分析

⑴系爭產品與系爭專利請求項1要件編號1A之均等比對

①就方式而言，如前述，系爭產品係藉由使用者的生物特徵解鎖儲存在行動裝置的私鑰後，由該私鑰對FIDO伺服器提供之亂數進行亂數運算，並將該亂數運算之結果傳回到該伺服器進行驗證，其中，該伺服器並未儲存使用者生物特徵的相關訊息，而系爭專利請求項1係藉由使用者本身具有唯一的生物特徵與儲存該生物特徵相關訊息的認證伺服主機進行該使用者身分的驗證，兩者使用的身分驗證技術明顯不同亦非可簡單置換，具有實質差異。

②就功能而言，系爭產品與系爭專利請求項1皆可提供使用者身分電子驗證之相同功能。

③就結果而言，系爭產品與系爭專利請求項1皆可達經由使用者之身分電子驗證確認使用者身分之相同結果。

④依上述，系爭產品要件編號1a與系爭專利請求項1要件編號1A，係以不同方式而獲得相同功能與結果，未構成均等，無法為系爭專利請求項1要件編號1A均等讀取。

⑵系爭產品與系爭專利請求項1要件編號1D、1E均等比對

①就方式而言，如前述，系爭產品係藉由使用者的生物特徵解鎖儲存在行動裝置的私鑰後，由該私鑰對FIDO伺服器提供之亂數進行亂數運算，並將該亂數運算之結果傳回到該伺服器進行驗證，而系爭專利請求項1係藉由編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼，並將該待驗證碼傳送至認證伺服主機進行驗證，兩者產生待驗證之內容，即系爭產品之「亂數運算之結果」、系爭專利請求項1之「待驗證碼」，其技術明顯不同亦非可簡單置換，具有實質差異。

②就功能而言，系爭產品之「亂數運算之結果」與系爭專利請求項1之「待驗證碼」，皆可提供使用者身分電子驗證之相同功能。

③就結果而言，系爭產品之「亂數運算之結果」與系爭專利請求項1之「待驗證碼」，皆可達經由使用者之身分電子驗證確認使用者身分之相同結果。

④依上述，系爭產品要件編號1d、1e與系爭專利請求項1要件編號1D、1E，係以不同方式而獲得相同功能與結果，未構成均等，無法為系爭專利請求項1要件編號1D、1E均等讀取。

⑶綜上，系爭產品未為系爭專利請求項1之要件編號1A、1D、1E均等讀取，故系爭產品亦未落入系爭專利請求項1之均等範圍。

6.系爭產品並不具有系爭專利請求項1要件編號1A、1D、1E之技術特徵，未落入系爭專利請求項1之文義範圍及均等範圍，已如前述，因系爭專利請求項2至8為系爭專利請求項1直接或間接依附之附屬項，故系爭產品亦未落入系爭專利請求項2至8之文義範圍及均等範圍。

7.原告另稱：使用者登錄/註冊時，須輸入生物特徵，並以之綁定一組公鑰及私鑰，私鑰用來加密而公鑰用來解密，彼此是唯一的，因此公鑰即與該生物特徵相關云云（見本院卷一第108頁）。惟查：

⑴依據系爭專利請求項1記載「使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證，其中該認證伺服主機係儲存與該生物特徵相關的訊息」，即系爭專利請求項1係藉由使用者本身唯一的生物特徵與認證伺服主機進行身分電子驗證。

⑵依據系爭專利說明書第7至8頁記載「本發明之虛實身分驗證電路、系統及電子消費方法，係可提供使用者藉由該虛實身分驗證電路將本身的生物特徵，經由複數種處理程序之至少其一者的演算而形成基於該生物特徵的該生物特徵碼，而該生物特徵碼係可透過遠端的認證伺服主機進行該使用者的身分電子驗證，而該認證伺服主機係可驗證該生物特徵碼是否符合在該認證伺服主機所存放與該使用者相關的該生物特徵」、第12頁記載「認證伺服主機24係包含資料庫單元242、收發單元244、驗證單元246與回饋單元248……資料庫單元242係儲存例如指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者的該生物特徵BC」，亦可知系爭專利係基於使用者本身的生物特徵與遠端認證伺服主機存放與該使用者相關的該生物特徵進行身分之驗證，即系爭專利請求項1所記載「生物特徵相關的訊息」係指如指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者的相關生物特徵。

⑶另依原告於本訴過程所稱「技術特徵1A明確描述伺服主機儲存生物特徵資訊……明確提及使用者透過其『唯一的生物特徵』與認證伺服主機進行驗證」（見本院卷二第17頁），即系爭專利請求項1所記載「生物特徵相關的訊息」係指使用者之相關生物特徵。

⑷綜上，原告所稱「公鑰」可對應「生物特徵相關的訊息」已逸脫系爭專利請求項1所界定之範圍，原告上開所稱並不足採。

8.原告復稱：編碼一詞，在程式設計中屬於廣義的定義，意指寫程式來解決特定的問題，所以在系爭專利請求項1要件

編號1D中，編碼可以涵蓋程式設計中的各種運算，比對可以稱做編碼（廣義）云云（見本院卷一第119至120頁）。惟查：依據系爭專利請求項1記載「處理單元係基於該處理程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼」，可知處理單元係將驗證金鑰碼與生物特徵碼進行編碼處理程序以產生相對應的待驗證碼，並未界定「編碼」可涵蓋「比對」之相關技術內容。另依系爭專利說明書第10至11頁記載「處理單元16係基於該處理程序DP處理該驗證金鑰碼VKC與該生物特徵碼BCC而產生相對應的待驗證碼UVC(unverified code)。再者，該處理程序DP係進一步可為以下的態樣：1)該處理程序DP係比對該生物特徵碼BCC與該驗證金鑰碼VKC用以決定是否產生該待驗證碼UVC；2)該處理程序DP對該生物特徵碼BCC與該驗證金鑰碼VKC進行編碼，用以產生相對應或包含該生物特徵碼BCC與該驗證金鑰碼VKC的該待驗證碼UVC」，亦可知系爭專利所述之「比對」係用以決定是否產生該待驗證碼，而「編碼」係用以產生該待驗證碼，兩者係屬不同作用。綜上，原告所稱並不足採。

六、專利有效性部分

㈠乙證2不足以證明系爭專利請求項1至8不具新穎性

乙證2為美國公告第5280527號「用於授權存取主機系統的生物特徵標記」專利案，公告日為西元1994年1月18日，早於系爭專利公告日（2017年1月11日），為系爭專利先前技術。

1.乙證2技術簡介

⑴技術內容

乙證2係涉及一種用於授權存取主機系統的生物特徵標記，其藉由一個安全裝置接收來自使用者的生物特徵輸入，然後將其與模板進行比較以確定相關係數，相關係數、固定碼以及時間變動碼或挑戰碼將被結合以生成一個標記，該標記顯示給使用者，使用者隨後將標記輸入

到存取裝置中，而存取裝置連接到安全主機系統，該存取裝置將標記轉發給主機，主機處理該標記以確定是否允許存取（摘譯自乙證2摘要，見本院卷一第529頁）。

⑵圖式

乙證2圖式如附圖3所示，其中圖1是乙證2包括生物特徵安全裝置之安全系統的示意圖；圖2是乙證2生物特徵安全裝置的示意圖（見本院卷一第530頁）。

2.系爭專利請求項1與乙證2之比對說明

⑴乙證2請求項1第1至3行記載「一種使用者驗證裝置，其用於驗證遠端主機系統的使用者的身分是否為授權使用者」、說明書第1欄第6至13行記載「本發明涉及一種用於接受生物特徵測量的裝置，然後此生物特徵測量可作為產生安全標記的種子。此標記被傳送到主機系統，以決定是否授權存取此主機」、說明書第2欄第48至51行記載「在本發明的一例示性實施例中，生物特徵安全機制是包括處理單元、記憶體及生物特徵感測器的積體電路卡」、說明書第3欄第29至34行記載「存取裝置可以是與主機電腦通訊的終端機、與具有主機資料庫管理系統的銀行網路通訊的自動櫃員機、與電腦系統連結的電話，甚至是限制存取安全區域的電子鎖」、說明書第6欄第35至45行記載「接著會顯示所導出的標記。使用者接著從顯示器20讀取標記，並在存取裝置12輸入標記。存取裝置12將標記傳送到主機10，主機10將標記解密或解碼，以導出固定碼及相關係數。如果固定碼識別出有效使用者，且相關係數高於臨界值，則允許存取。如果不是，則會拒絕存取。有了用於識別特定個人或群組的固定碼，主機可經程式化以控制此固定碼所允許的存取或交易類型」，其中所述之「生物特徵安全機制」、「存取裝置」、「主機系統」可對應系爭專利請求項1之「虛實身分驗證電路」、「電子裝置」、「認證伺服主機」，故乙證2已揭示系爭專利請求項1「一種虛實身

分驗證電路，係供內建於電子裝置或與該電子裝置連接，用以讓使用者藉由本身具有唯一的生物特徵與位於網際網路的認證伺服主機進行該使用者的身分電子驗證」之技術特徵。

⑵乙證2請求項1第1至9行記載「一種使用者驗證裝置，其用於驗證遠端主機系統的使用者的身分是否為授權使用者，包含：…(b)記憶體構件，用於儲存接受受臨界值層級資料，以及先前取得的授權使用者生物特徵資訊和固定碼」、說明書第1欄第28至37行記載「常見的安全機制包括使用個人識別碼（PIN）和使用安全標記。PIN用於識別個人身份並授權存取主機系統（例如銀行交易系統）。安全標記是由私鑰（例如：獨特的固定值）和公鑰（例如：時間變動值）導出的不可預測碼。舉例來說，密碼（固定金鑰）會根據時間變動資訊進行編碼。然後，此種標記會被轉送至主機，由主機將標記解碼回密碼」，其中所述之「記憶體構件」、「固定碼」可對應系爭專利請求項1之「記憶單元」、「驗證金鑰碼」，故乙證2已揭示系爭專利請求項1「記憶單元，係具有儲存空間，該儲存空間儲存驗證金鑰碼」之技術特徵。

⑶乙證2請求項1記載「一種使用者驗證裝置，其用於驗證遠端主機系統的使用者的身分是否為授權使用者，包含：(a)用於從該使用者接收生物特徵資訊之構件……(c)比較構件，用於將來自該使用者的該生物特徵資訊與該先前取得的生物特徵資訊進行比較並產生相關係數」、說明書第5欄第42至54行記載「生物特徵感測器18偵測來自使用者（即持卡人、持筆人）的生物特徵輸入，其確切性質對本發明來說並不重要，只要它感測到的資訊基本上是個人資訊，並且所偵測到的特徵實質不變即可。根據各種實施例，感測器18可以偵測指紋、簽章、語音或其他類似資訊。對於卡片實施例1

4’，感測器18可以是偵測指紋的掃描裝置或是偵測簽章的壓力感測裝置。或者也可以使用CCD成像裝置來擷取指紋或簽章的圖片。感測器18還可以是語音偵測器」，其中所述之「生物特徵感測器」、「生物特徵資訊」可對應系爭專利請求項1之「擷取單元」、「生物特徵碼」，故乙證2已揭示系爭專利請求項1「擷取單元，係供擷取該生物特徵，該擷取單元係根據擷取的該生物特徵產生相對應的生物特徵碼，其中該擷取單元可透過指紋辨識器或攝影機擷取該生物特徵」之技術特徵。

⑷乙證2請求項2記載「如請求項1所述之裝置，其中該訊號產生構件進一步適於將該第一認證碼和該固定碼結合以產生可傳輸碼，該可傳輸碼適於傳輸至該傳輸構件，以便隨後傳輸至該主機系統，以便由該主機系統決定是否允許該使用者存取該主機系統」、請求項3記載「如請求項2所述之裝置，其進一步包括用於將時間變動碼輸入該記憶體構件之構件，且其中該訊號產生構件適於結合該第一驗證碼與該時間變動碼以產生可傳輸碼，該可傳輸碼適於傳輸至該傳輸構件，以便隨後傳輸至該主機系統，以便由該主機系統決定是否允許該使用者存取該主機系統」，即乙證2已揭示可將認證碼和固定碼結合以產生可傳輸碼抑或時間變動碼結合第一驗證碼產生可傳輸碼，其中所述之「時間變動碼」可對應系爭專利請求項1之「動態金鑰碼」，儲存至記憶單元而形成驗證金鑰碼，故乙證2已揭示系爭專利請求項1「其中該通訊單元係接收動態金鑰碼並將該動態金鑰碼儲存至該記憶單元而在該記憶單元形成該驗證金鑰碼，且該動態金鑰碼是被動式更換或主動式更換」之技術特徵。

⑸乙證2並未揭示系爭專利請求項1「認證伺服主機係儲存與該生物特徵相關的訊息」（下稱「差異技術特徵1A」）、「處理單元，係連接該記憶單元與該擷取單元，該處理單元係具有處理程序，且該處理單元係基於該處

理程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼，其中該待驗證碼具有該生物特徵碼與該驗證金鑰碼之至少一者」(下稱「差異技術特徵1D」)、「通訊單元，係與該處理單元連接，該通訊單元將該待驗證碼傳送至該網際網路，以及等待該認證伺服主機回傳與該待驗證碼相關該身分電子驗證的驗證結果」(下稱「差異技術特徵1E」)之技術特徵。

3.依上述，乙證2因未揭示系爭專利請求項1之全部技術特徵，故不足以證明系爭專利請求項1不具新穎性。

4.系爭專利請求項2至8為系爭專利請求項1直接或間接依附之附屬項，乙證2不足以證明系爭專利請求項1不具新穎性，已如前述，故乙證2亦不足以證明系爭專利請求項2至8不具新穎性。

㈡乙證2不足以證明系爭專利請求項1至8不具進步性

1.乙證2並未揭示系爭專利請求項1之「差異技術特徵1A」、「差異技術特徵1D」、「差異技術特徵1E」，已如前述。另乙證2說明書第6欄第35至45行雖揭示主機10可將標記解密或解碼，以導出相關係數，如果相關係數高於臨界值則允許存取，然依據乙證2請求項1記載可知，所述之「相關係數」係經由生物特徵資訊與該先前取得的生物特徵資訊進行比較後產生，難謂該「相關係數」可對應系爭專利請求項1之「生物特徵相關的訊息」，再者，乙證2之主機10亦僅揭示一臨界值，亦非系爭專利請求項1認證伺服主機儲存之「生物特徵相關的訊息」。

2.另依據乙證2請求項1、2、3可知，相關係數與接受臨界值層級資料進行比較後產生一可傳輸碼，該可傳輸碼包括認證碼、固定碼、時間變動碼，然該可傳輸碼與系爭專利請求項1所述藉由編碼驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼，兩者產生的方式並不相同。

3.依上述，系爭專利請求項1之「差異技術特徵1A」、「差異技術特徵1D」、「差異技術特徵1E」並非該發明所屬技

術領域中具有通常知識者依乙證2之內容所能預期者，自非屬依據申請前之先前技術所能輕易完成，故乙證2亦不足以證明系爭專利請求項1不具進步性。

4.系爭專利請求項2至8為系爭專利請求項1直接或間接依附之附屬項，乙證2不足以證明系爭專利請求項1不具進步性，已如前述，故乙證2亦不足以證明系爭專利請求項2至8不具進步性。

㈢乙證2、3之組合足以證明系爭專利請求項1至8不具進步性

1.乙證3技術簡介

乙證3為韓國公開第20010016395號「基於網際網路的使用指紋的會員管理系統和方法」專利案，公告日為2001年3月5日，早於系爭專利公告日（2017年1月11日），為系爭專利先前技術。

⑴技術內容

乙證3係關於一種基於網際網路的使用指紋的會員管理系統和方法，透過連接至網際網路的指紋識別伺服器系統與各加盟店的客戶端系統，利用指紋此辨識性極佳的生物特徵辨識手段，對使用者的身分進行辨識與認證(摘譯自乙證3摘要，本院卷一第537頁)。

⑵圖式

乙證3圖式如附圖4所示，其中圖1是乙證3基於網際網路的指紋會員管理系統示意圖。

2.系爭專利請求項1與乙證2、3之比對說明

⑴乙證2並未揭示系爭專利請求項1之「差異技術特徵1A」、「差異技術特徵1D」、「差異技術特徵1E」，已如前述。另查，乙證3第10-3頁第4段記載「…為了識別客戶是否是會員，系統利用指紋資訊（一種識別個人的高效生物特徵識別構件）來識別和驗證會員(2)的身份。透過與網際網路連結的會員管理網路伺服器系統(1)對在各商家或商店註冊的會員(2)進行整體管理，因此，會員客戶只需使用指紋，即可在實施根據本發明服

務的商家或商店獲得離線里程優惠，並透過網際網路存取會員管理網路伺服器系統(1)，以獲得各種資訊與優惠，是一種兼顧客戶利益和便利性的會員管理系統」、第10-4頁第7及8段記載「圖1是根據本發明之一實施例所配置的整體區塊圖。會員管理伺服器系統(1)是根據本發明服務的主體，其包括網路伺服器單元(10)及資料庫伺服器單元(20)」、第10-5頁第6段記載「資料庫伺服器單元(20)包括會員資訊資料庫單元(21)及指紋資訊資料庫單元(22)…指紋資訊資料庫單元(22)將實施本發明服務的商家或商店所註冊的會員的指紋微特徵提取資訊進行分類和儲存，並在透過顧客指紋資訊進行會員認證請求時，驗證其是否與註冊會員的指紋資訊相符」、請求項1記載「一種基於網際網路的使用指紋的會員管理系統和方法中，包括：…第四步驟，在會員管理伺服器單元的接收單元接收從用戶端單元經由網際網路傳輸的資料，在指紋識別單元中以預設的密鑰進行解密，識別用戶端單元的唯一識別碼和使用者的指紋微特徵資訊，並搜尋資料庫伺服器單元以檢查是否存在相應記錄」、請求項3記載「一種基於網際網路的使用指紋的會員管理系統和方法中，包括：…一資料庫伺服器單元，包括一會員資訊資料庫單元，用於儲存會員的個人資訊，以驗證連結至會員管理伺服器單元的會員身份；以及一指紋資訊資料庫單元，用於分類及儲存指紋資訊，以在指紋辨識單元中搜尋與使用者指紋微特徵資訊相符的會員指紋資訊，其特徵為一基於網際網路的使用指紋的會員管理系統」，其中所述之「用戶端單元」、「會員管理伺服器系統」、「指紋」可對應系爭專利請求項1之「虛實身分驗證電路，係內建於電子裝置」、「認證伺服主機」、「生物特徵相關的訊息」，故乙證3已揭示系爭專利請求項1之「差異技術特徵1A」。

⑵乙證3第10-5頁第13段記載「客戶透過用戶端單元(30)指紋輸入單元(31)輸入指紋，例如獨立的指紋輸入裝置或帶有指紋輸入裝置(200)的鍵盤或滑鼠。透過指紋輸入單元(31)輸入的指紋影像經由指紋微特徵提取模組(32)中的指紋微特徵提取演算法處理，以提取客戶的唯一指紋微特徵，例如紋脊末端和分叉(210)。將客戶的指紋微特徵資訊和商家或商店的唯一識別碼經由預設的密鑰加密後，轉換為封包形式的資料，透過通訊單元(220)傳輸並與會員管理伺服器單元(10)形成會話」、請求項1記載「…第一步驟，透過連接至網際網路的用戶端單元的指紋輸入單元輸入使用者的指紋；第二步驟，使用指紋微特徵提取模組中的指紋微特徵提取演算法，從第一步驟輸入的使用者指紋影像中，提取使用者的唯一指紋微特徵」、請求項3記載「…一指紋輸入單元，用於掃描使用者的指紋，並將其轉換成一數位指紋影像，以便於在指紋微特徵提取模組進行處理；以及一指紋微特徵提取模組，用於使用指紋微特徵提取演算法，從經由指紋輸入單元輸入的指紋影像中，提取使用者的唯一指紋微特徵」，其中所述之「指紋輸入單元」、「指紋微特徵」、「將客戶的指紋微特徵資訊和商家或商店的唯一識別碼經由預設的密鑰加密」、轉換為「封包形式的資料」可對應系爭專利請求項1之「擷取單元」、「生物特徵碼」、「基於處理程序編碼該驗證金鑰碼與該生物特徵碼而產生相對應的待驗證碼」、「待驗證碼」，故乙證3已揭示系爭專利請求項1之「差異技術特徵1D」。

⑶乙證3第10-4頁第10段記載「用戶端單元(30)包括指紋輸入單元(31)、指紋微特徵提取模組(32)、網頁瀏覽器單元(33)以及通訊單元(34)」、第10-5頁第13段記載「將客戶的指紋微特徵資訊和商家或商店的唯一識別碼經由預設的密鑰加密後，轉換為封包形式的資料，透過

通訊單元(220)傳輸並與會員管理伺服器單元(10)形成會話」、請求項1記載「第四步驟，在會員管理伺服器單元的接收單元接收從用戶端單元經由網際網路傳送的資料，在指紋識別單元中以預設密鑰進行解密，識別用戶端單元的唯一識別碼和使用者的指紋微特徵資訊，並搜索資料庫伺服器單元，檢查是否存在相應記錄；第五步驟，若有符合使用者指紋的記錄，則透過網際網路將該使用者的個人資訊、里程使用記錄，以及該使用者是否註冊為用戶端單位的會員的資訊傳送至用戶端單元」，其中所述之「將該使用者的個人資訊、里程使用記錄，以及該使用者是否註冊為用戶端單位的會員的資訊傳送至用戶端單元」可對應系爭專利請求項1之「回傳與該待驗證碼相關該身分電子驗證的驗證結果」，故乙證3已揭示系爭專利請求項1之「差異技術特徵1E」。

⑷乙證2及乙證3皆屬於身分驗證資料處理之技術領域，且兩者皆涉及如何利用使用者本身唯一的生物特徵進行安全身分驗證，具有技術領域之關連性、欲解決問題之共通性、及作用或功能之共通性。故對於所屬技術領域中具有通常知識者，在基於乙證2之基礎下，自有動機將乙證3揭示的「指紋」作為乙證2使用者與主機系統身分驗證的資訊，以完成系爭專利請求項1之全部技術特徵，故乙證2、3之組合足以證明系爭專利請求項1不具進步性。

3.系爭專利請求項2、3與乙證2、3之比對說明

系爭專利請求項2、3為系爭專利請求項1之直接或間接之附屬項，乙證2、3之組合足以證明系爭專利請求項1不具進步性已如前述。另查，乙證2請求項1記載「一種使用者驗證裝置……包含：…(b)記憶體構件，用於儲存接受臨界值層級資料，以及先前取得的授權使用者生物特徵資訊…(c)比較構件，用於將來自該使用者的該生物特徵資訊與該先前取得的生物特徵資訊進行比較並產生相關係

數；(d)訊號產生構件，用於將該相關係數與該接受臨界值層級資料進行比較以產生可傳輸碼，該可傳輸碼包括認證碼」，即乙證2已揭示在產生可傳輸碼前，需先將來自使用者的生物特徵資訊與先前取得的生物特徵資訊進行比較，其中所述之「先前取得的授權使用者生物特徵資訊」可對應系爭專利請求項2之「本地驗證金鑰」及系爭專利請求項3之「該驗證金鑰碼」，是乙證2已揭示系爭專利請求項2、3所進一步界定「其中該記憶單元係為預先地儲存與該生物特徵相關的本地驗證金鑰」、「其中該處理單元係在基於該處理程序比對該生物特徵碼與該驗證金鑰碼，用以決定是否產生該待驗證碼」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項2、3不具進步性。

4.系爭專利請求項4與乙證2、3之比對說明

系爭專利請求項4為系爭專利請求項1之附屬項，乙證2、3之組合足以證明系爭專利請求項1不具進步性已如前述。乙證3已揭示客戶的指紋微特徵資訊和商家或商店的唯一識別碼經由預設的密鑰加密，其中所述之「唯一識別碼」可對應系爭專利請求項4之「與電子裝置相關的驗證金鑰碼」，是乙證3已揭示系爭專利請求項4所進一步界定「其中該記憶單元係為儲存與該電子裝置相關的該驗證金鑰碼，用於供該處理單元基於該處理程序編碼該生物特徵碼與該驗證金鑰碼以產生相對應於該生物特徵碼與該驗證金鑰碼的該待驗證碼」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項4不具進步性。

5.系爭專利請求項5與乙證2、3之比對說明

系爭專利請求項5為系爭專利請求項4之附屬項，乙證2、3之組合足以證明系爭專利請求項4不具進步性已如前述。另查，乙證2說明書第2欄第55至59行記載「驗證演算法使用模板資料、生物特徵輸入、固定碼（即PIN、嵌入式序號、帳號）和隨時間變化的自生成資訊來導出標記輸出」，即乙證2已揭示固定碼可為PIN、嵌入式序號、帳號

等，其中所述之「PIN」可對應系爭專利請求項5之「用戶自訂密碼」，是乙證2已揭示系爭專利請求項5所進一步界定「其中該驗證金鑰碼係為來自於該電子裝置的媒體存取控制位址(Media Access Control Address)、用戶身份模塊(Subscriber Identity Module)與用戶自訂密碼之至少其一者」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項5不具進步性。

6.系爭專利請求項6與乙證2、3之比對說明

系爭專利請求項6為系爭專利請求項1之附屬項，乙證2、3之組合足以證明系爭專利請求項1不具進步性已如前述。另查，乙證2說明書第5欄第42至54行記載「生物特徵感測器18偵測來自使用者（即持卡人、持筆人）的生物特徵輸入，其確切性質對本發明來說並不重要，只要它感測到的資訊基本上是個人資訊，並且所偵測到的特徵實質不變即可。根據各種實施例，感測器18可以偵測指紋」，即乙證2已揭示生物特徵可為指紋，可對應系爭專利請求項6所進一步界定「其中該生物特徵係指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項6不具進步性。

7.系爭專利請求項7與乙證2、3之比對說明

系爭專利請求項7為系爭專利請求項1之附屬項，乙證2、3之組合足以證明系爭專利請求項1不具進步性已如前述。另查，乙證2說明書第4欄第15至22行記載「在一替代實施例中，安全裝置14直接耦合至主機系統10，使得標記輸出可直接傳輸至主機，而無需顯示標記或由使用者手動輸入。例如，可以使用標準資料通訊電纜或任何其他已知的資料傳輸技術完成此耦合」，即乙證2已揭示可使用標準資料通訊電纜或任何其他已知的資料傳輸技術進行資料傳輸，可對應系爭專利請求項7所進一步界定「其中該通訊單元係以有線通訊型態或是無線通訊型態傳送該待驗證

碼」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項7不具進步性。

8.系爭專利請求項8與乙證2、3之比對說明

系爭專利請求項8為系爭專利請求項1之附屬項，乙證2、3之組合足以證明系爭專利請求項1不具進步性已如前述。乙證2已揭示可使用標準資料通訊電纜或任何其他已知的資料傳輸技術進行資料傳輸，又對於所屬技術領域中具有通常知識者可知，以藍芽(Bluetooth)、固網通訊、行動通訊、無線保真(Wi-Fi)的通訊協定進行資料傳輸，已為所屬技術領域之通常知識，是乙證2可對應系爭專利請求項8所進一步界定「其中該通訊單元係符合藍芽(Bluetooth)、固網通訊、行動通訊、無線保真(Wi-Fi)的通訊協定」之技術特徵，故乙證2、3之組合足以證明系爭專利請求項8不具進步性。

㈣乙證2、4之組合足以證明系爭專利請求項1至8不具進步性

1.乙證4技術簡介

乙證4為美國公開第2011/0191250號「進行電子交易的方法和裝置」專利案，公告日為2011年8月4日，早於系爭專利公告日（2017年1月11日），為系爭專利先前技術。

⑴技術內容

乙證4係關於一種利用智慧型儀器進行電子交易的系統與方法，授權伺服器透過向智慧型儀器的智慧型標記發出質詢，智慧型標記產生質詢回應並將其傳送至授權伺服器，該伺服器在驗證回應後，組合包含電子交易金鑰的憑證，授權伺服器將組合後的憑證傳送至智慧型儀器，智慧型儀器在後續交易中將該憑證傳送至授權伺服器，授權伺服器驗證該憑證，並在驗證成功後對交易提供授權（摘譯自乙證4摘要，見本院卷一第547頁）。

⑵圖式

乙證4圖式如附圖5所示，其中圖1C是乙證4交易系統的示意圖；圖10是乙證4登入序列的訊息序列圖（見本院

卷一第548頁)。

2.系爭專利請求項1與乙證2、4之比對說明

⑴乙證2並未揭示系爭專利請求項1之「差異技術特徵1A」、「差異技術特徵1D」、「差異技術特徵1E」，已如前述。另查，乙證4說明書第[0002]段記載「本發明一般涉及進行網路交易的方法與裝置。更特別的是，本發明涉及使用個人識別符（例如生物特徵）在資料網路（例如網際網路）上驗證和進行交易的系統」、第[0102]段記載「在各種實施例中，讀卡機204與客戶電腦110互動，以提示使用者提供個人識別符，例如個人識別碼(PIN)或其他唯一識別符，以存取卡片。在一例示性實施例中，PIN儲存在智慧型儀器202上」、第[0104]段記載「在接收到回應訊息1008之後，安全伺服器130對此訊息進行適當的處理（圖10中的步驟1010)。在各種實施例中，回應訊息1008被路由至授權伺服器306，授權伺服器306驗證智慧型儀器202提供的憑證與簽章。在成功驗證憑證和簽章的有效性後，在各種實例中，可產生安全標記並將其傳回給客戶110或智慧型儀器202」、第[0253]段記載「在一實施例中，如上文進一步詳細說明明，生物特徵樣本可用作產生公鑰/私鑰對的基礎。例如，可以使用基於生物特徵樣本的私鑰加密質詢回應，並使用相對應的公鑰解密。換句話說，質詢回應可以使用基於生物特徵樣本資料產生或植入的加密金鑰進行數位簽章。此外，可以使用公鑰來加密與質詢回應相關的資料。亦即不是用基於生物特徵樣本的私鑰加密質詢回應以形成數位簽章，而是可以用基於生物特徵樣本的公鑰加密包含質詢回應的資料。在這種情況下，當然可以在伺服器上使用相對應的私鑰來解密資料。因此，生物特徵樣本在用戶端既可用作私鑰，也可用作公鑰，其取決於它是用作數位簽章的基礎還是用作加密資料的基礎，以確保資料的安全性除了預期的接收者之外，其他

人都無法收到訊息」，其中所述之「智慧型儀器」、「客戶電腦」、「授權伺服器」、「生物特徵樣本」可對應系爭專利請求項1之「虛實身分驗證電路」、「電子裝置」、「認證伺服主機」、「生物特徵相關的訊息」，又乙證4已揭示生物特徵樣本可用作產生公鑰與私鑰對的基礎，可以使用基於生物特徵樣本的私鑰加密質詢回應，並使用相對應的公鑰解密，亦即伺服器上儲存有基於生物特徵樣本的公鑰(或私鑰)，故乙證4已揭示系爭專利請求項1之「差異技術特徵1A」。

⑵乙證4說明書第[0119]段記載「智慧型儀器讀取器204可配有生物特徵感測器1604，在此進一步詳述。智慧型儀器202可經由智慧型儀器讀取器204與網路102進行通訊」、第[0122]段記載「如本文所用，可以用多種方式處理生物特徵以建立生物特徵樣本。例如，虹膜之生物特徵讀取會產生生物特徵，其中，當處理生物特徵讀取經處理以建立虹膜的數位表示時，會建立生物特徵樣本」、第[0247]段記載「據此，使用者向智慧型儀器202提供生物特徵樣本，智慧型儀器202將此生物特徵樣本轉換為生物特徵資料並傳輸至授權伺服器306」、第[0141]段記載「生物特徵安全系統1402可包括生物特徵感測器1404，其可經配置有視訊攝影機、光學掃描器、成像雷達、紫外線成像及/或其他硬體及/或軟體，用於從人身上擷取生物特徵資料」、第[0101]段記載「例如，錢包用戶端214可以提取伺服器質詢資訊，格式化新的用戶端質詢（即，智慧型儀器202的第二個加密質詢），將兩個質詢組合成雙重質詢，並計算雙重質詢的雜湊值以供之後使用，例如，在公鑰密碼系統1(PKCS1)密碼區塊中」、第[0102]段記載「PKCS1區塊透過讀卡機204適當地提供給智慧型儀器202進行處理（圖10中的步驟1006)。在各種實施例中，讀卡機204與客戶電腦110互動，以提示使用者提供個人識別符，例如個人識別

碼(PIN)或其他唯一識別符，以存取卡片。在一例示性實施例中，PIN儲存在智慧型儀器202上。或者，PIN或其他個人識別符可以儲存在系統的其他地方，例如讀卡機204或客戶電腦110上。使用者適當地輸入個人識別符以解鎖智慧型儀器202，智慧型儀器202從錢包用戶端214接收雙重質詢區塊，並適當地對區塊進行數位簽章。在各種實施例中，智慧型儀器202包含用於計算區塊數位簽章的密鑰。經簽署的區塊會視情況傳回至錢包用戶端214。在各種實施例中，智慧型儀器202也提供與用於計算數位簽章的私鑰對應的憑證」、第[0103]段記載「在從智慧型儀器202接收到簽章和憑證後，錢包用戶端214適當地建立適當的回應訊息1008以傳送給安全伺服器130」，其中所述之「生物特徵感測器」、「生物特徵資料」、「視訊攝影機、光學掃描器、成像雷達、紫外線成像」可對應系爭專利請求項1之「擷取單元」、「生物特徵碼」、「指紋辨識器」，又依據前述乙證4說明書第[0253]段記載可知，乙證4已揭示生物特徵樣本可用作產生公鑰與私鑰對的基礎，可以使用基於生物特徵樣本的私鑰加密質詢回應，質詢回應可以使用基於生物特徵樣本資料產生或植入的加密金鑰進行數位簽章，而所述之「使用基於生物特徵樣本的私鑰加密質詢回應」、「質詢」、「數位簽章」可對應系爭專利請求項1之「編碼該驗證金鑰碼與該生物特徵碼」、「驗證金鑰碼」、「待驗證碼」，故乙證4已揭示系爭專利請求項1之「差異技術特徵1D」。

⑶乙證4說明書第[0103]段記載「在從智慧型儀器202接收簽章和憑證後，錢包用戶端214適當地建立適當的回應訊息1008以傳送給安全伺服器130」、第[0104]段記載「在接收到回應訊息1008之後，安全伺服器130對此訊息進行適當的處理（圖10中的步驟1010）。在各種實施例中，回應訊息1008被路由到授權伺服器306，授權伺

服器306驗證智慧型儀器202提供的憑證和簽章。在成功驗證憑證和簽章的有效性後，在各種實施例中，可以產生安全標記並將其傳回給客戶110或智慧型儀器202」，其中所述之「產生安全標記並將其傳回給客戶110或智慧型儀器202」可對應系爭專利請求項1之「回傳與該待驗證碼相關該身分電子驗證的驗證結果」，故乙證4已揭示系爭專利請求項1之「差異技術特徵1E」。

⑷乙證2及乙證4皆屬於身分驗證資料處理之技術領域，且兩者皆涉及如何利用使用者本身唯一的生物特徵進行安全身分驗證，具有技術領域之關連性、欲解決問題之共通性、及作用或功能之共通性。故對於所屬技術領域中具有通常知識者，在基於乙證2之基礎下，自有動機將乙證4揭示的「生物特徵」作為乙證2使用者與主機系統身分驗證的資訊，以完成系爭專利請求項1之全部技術特徵，故乙證2、4之組合足以證明系爭專利請求項1不具進步性。

3.系爭專利請求項2至8為系爭專利請求項1之直接或間接的附屬項，乙證2、4之組合足以證明系爭專利請求項1不具進步性已如前述。另如前述，乙證2已揭示可對應系爭專利請求項2、3、5至8所進一步界定之技術特徵，再查，乙證2第4欄第50行至第5欄第14行記載「在一實施例中，處理器22是8位元微處理器，晶片上具有156位元組隨機存取記憶體，例如由加州聖克拉拉市的英特爾公司製造的8051型微處理器……每個安全裝置14都附有嵌入式的『固定』碼，儲存在PROM24中」，其中所述之「嵌入式的『固定』碼」可對應系爭專利請求項4之「與電子裝置相關的驗證金鑰碼」，是乙證2、4已揭示系爭專利請求項4所進一步界定之技術特徵。

4.綜上，乙證2、4之組合足以證明系爭專利請求項2至8不具進步性。

㈤對原告陳述之意見

1.原告稱：乙證2並未提及感測器產收生物特徵碼以及如何產生生物特徵碼云云（見本院卷二第279至281頁）。惟查，乙證2請求項1已揭示可將來自該使用者的該生物特徵資訊與該先前取得的生物特徵資訊進行比較並產生相關係數，對於所屬技術領域中具有通常知識者當可知，乙證2之生物特徵感測器於偵測來自使用者的生物特徵輸入後，為與該先前取得的生物特徵資訊進行比較，需將該生物特徵轉換成數位之生物特徵資訊，是該生物特徵資訊當可對應系爭專利之生物特徵碼，原告所述理由並不足採。

2.原告復稱：乙證3中的指紋微特徵資料只是從指紋影像中提取出的特徵點集合，而系爭專利中的生物特徵碼是經過特定算法處理後生成的一組不可逆識別碼；乙證3的「封包形式的資料」只是包含指紋微特徵與唯一識別碼的數據封裝，並未明確揭示這些數據會經過特定的處理程序來形成類似系爭專利的「待驗證碼」；系爭專利的通訊單元除了負責傳輸待驗證碼，還需等待該認證伺服主機回傳與該待驗證碼相關的驗證結果；系爭專利的認證伺服主機主要回傳的是該待驗證碼相關的身份電子驗證結果，而不是乙證3額外的個人資訊或使用記錄云云（見本院卷二第300至305頁）。惟查，系爭專利並未記載生物特徵碼是經過特定算法處理後生成的一組不可逆識別碼。另如前述，乙證3已揭示可將客戶的指紋微特徵資訊和商家或商店的唯一識別碼經由預設的密鑰加密後，轉換為封包形式的資料，其中所述形成「封包形式的資料」之過程即可對應系爭專利之「處理程序」，又對於所屬技術領域中具有通常知識者可知，該過程當由可對應系爭專利「處理器」之構件所執行。再者，系爭專利並未限定「驗證結果」之內容為何？而如前述，乙證3已揭示會員管理伺服器單元若檢查有符合使用者指紋的記錄，則透過網際網路將該使用者的個人資訊、里程使用記錄，以及該使用者是否註冊為用戶端單位的會員的資訊傳送至用戶端單元，即乙證3已揭示

會員管理伺服器單元會驗證使用者身分並回傳驗證之結果，又用戶端單元要接收會員管理伺服器單元回傳驗證之結果，當藉由其通訊單元接收。綜上所述，原告所稱並不足採。

3.原告又稱：乙證4未揭示「處理單元」如何連接「記憶單元」與「擷取單元」?「處理程序」如何將「驗證金鑰碼」與「生物特徵碼」進行編碼?「待驗證碼」是否確實包含驗證金鑰碼與生物特徵碼之一?乙證4並未揭露通訊單元的具體實作方式，例如：是否是一個獨立的網路模組云云（見本院卷二第313至316頁）。惟查，如前述，乙證4所述之「生物特徵感測器」可對應系爭專利請求項1之「擷取單元」，而生物特徵樣本可用作產生公鑰與私鑰對的基礎，可以使用基於生物特徵樣本的私鑰加密質詢回應，質詢回應可以使用基於生物特徵樣本資料產生或植入的加密金鑰進行數位簽章，其中所述形成「數位簽章」之過程即可對應系爭專利之「處理程序」，且該數位簽章當包含可對應原告所稱系爭專利「『驗證金鑰碼』與『生物特徵碼』之一」的「質詢」與「生物特徵樣本」之一者，又對於所屬技術領域中具有通常知識者可知，該過程當由可對應系爭專利「處理器」之構件所執行。另如前述，乙證4所述之「客戶電腦」可對應系爭專利請求項1之「電子裝置」，對於所屬技術領域中具有通常知識者可知，該「客戶電腦」當具有可對應系爭專利「記憶單元」之構件以儲存該生物特徵樣本，又乙證4已揭示授權伺服器驗證智慧型儀器提供的憑證和簽章，在成功驗證憑證和簽章的有效性後，可以產生安全標記並將其傳回給客戶或智慧型儀器，是乙證4當具有可對應系爭專利「通訊單元」之構件以傳送憑證/簽章及接收安全標記。據此，所屬技術領域中具有通常知識者可知，前述乙證4可對應系爭專利「擷取單元」、「處理器」、「記憶單元」、「通訊單

元」之構件當會具有協同運作以達成乙證4利用智慧型儀器進行電子交易的系統與方法，原告所稱理由並不足採。

4.原告再稱：乙證3的「唯一識別碼」不等於系爭專利請求項4的「驗證金鑰碼」，並非由生物特徵碼衍生的驗證金鑰碼；系爭專利請求項6之技術特徵「指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者」為明確限制，這些生物特徵中除語音與指紋外，其他在乙證2中並未提及；乙證2未揭露請求項7所要求的完整技術特徵，因為僅揭示「有線」通訊，未包含「有線或無線」的選擇性云云（見本院卷二第336至339、345、352頁）。惟查，依系爭專利請求項4之記載「其中該記憶單元係為儲存與該電子裝置相關的該驗證金鑰碼……」，可知該請求項之驗證金鑰碼係與電子裝置相關，並非所稱由生物特徵碼衍生。另查，系爭專利請求項6記載「其中該生物特徵係指紋、虹膜、掌紋、靜脈血管、語音與臉型之至少其一者」、請求項7記載「其中該通訊單元係以有線通訊型態或是無線通訊型態」，即系爭專利請求項6、7所進一步界定之技術特徵皆以擇一記載形式界定其附加之技術特徵，乙證2既已揭示其中擇一之態樣，即已揭示該進一步界定之技術特徵。綜上，原告所稱皆不足採。

七、綜上所述，系爭產品未落入系爭專利請求項1至8之文義及均等範圍。乙證2、3之組合及乙證2、4之組合均足以證明系爭專利請求項1至8不具進步性，依智慧財產案件審理法第41條第2項規定，原告不得以系爭專利對被告主張權利。從而，原告依專利法第96條第1項、第3項規定請求防止、排除被告侵害系爭專利，並將流通至市面上之系爭產品予以刪除，及依同法第96條第2項、第97條第1項規定請求被告賠償損害，為無理由，應予駁回。原告之訴既經駁回，其假執行之聲請失其依據，併予駁回。

八、本件事證已臻明確，兩造其餘攻擊防禦方法，於本件判決結果不生影響，爰不予一一論述，附此敘明。

據上論結，本件原告之訴無理由，依智慧財產案件審理法第2條，民事訴訟法第78條，判決如主文。

中　　華　　民　　國　　114　　年　　7　　月　　18　　日

智慧財產第二庭

法　官　李維心

以上正本係照原本作成。

如不服本判決，應於收受送達後20日內向本院提出上訴書狀，上訴時應提出委任律師或具有智慧財產案件審理法第10條第1項但書、第5項所定資格之人之委任狀；委任有前開資格者，應另附具各該資格證書及釋明委任人與受任人有上開規定（詳附註）所定關係之釋明文書影本。如委任律師提起上訴者，應一併繳納上訴審裁判費。

中　　華　　民　　國　　114　　年　　7　　月　　21　　日

書記官　林佳蘋

附註：

智慧財產案件審理法第10條第1項、第5項

智慧財產民事事件，有下列各款情形之一者，當事人應委任律師為訴訟代理人。但當事人或其法定代理人具有法官、檢察官、律師資格者，不在此限：

一、第一審民事訴訟事件，其訴訟標的金額或價額，逾民事訴訟法第四百六十六條所定得上訴第三審之數額。

二、因專利權、電腦程式著作權、營業秘密涉訟之第一審民事訴訟事件。

三、第二審民事訴訟事件。

四、起訴前聲請證據保全、保全程序及前三款訴訟事件所生其他事件之聲請或抗告。

五、前四款之再審事件。

六、第三審法院之事件。

七、其他司法院所定應委任律師為訴訟代理人之事件。

當事人之配偶、三親等內之血親、二親等內之姻親，或當事人為法人、中央或地方機關時，其所屬專任人員具有律師資格，並經

法院認為適當者，亦得為第一項訴訟代理人。