連宇股份有限公司

金融應用個人密碼辨識器

■計畫目標

金融應用個人密碼辨識器,依所定義之規格完成開發設計；為磁卡及 IC 卡的讀取機，提供磁卡資料解碼輸出及 IC 卡通訊架構之功能。金融應用個人密碼辨識器為一用來提供使用者輸入個人密碼並加以辨識、加密並傳輸至主機之周邊設備，主要運用於銀行金融系統 及零售業電子交易系統中。

其機構模組設計目標為

1. 符合人體工學 16 鍵橡皮鍵盤
2. 磁卡讀卡磁頭模組設計及晶片卡模組設計
3. 資料防竊感應設計
4. 密碼防窺視設計
5. 灌膠封裝設計

其硬體設計目標為

1. 安全保護機制
   企圖打開機蓋的動作，會使得內部的記憶體消除，以達到保護的目的。
2. 模組化設計
   模組化設計，使得金融應用個人密碼辨識器可以擁有更多的更換模組，目前已有純磁卡功能，及含有IC晶片卡和磁條卡等功能的選擇，搭配不同的輸入介面，未來將有八種組合之多。
3. 使用傳統之 RS232 介面，並加入新一代的 USB傳輸介面
   設計 USB 模組，直接接入金融應用個人密碼辨識器中，便可達到USB 傳輸介面的功能
4. 內建LDO (Low Dropout Regulators) regulator
   使得輸入電壓不僅限於 9V,也具有過電流保護功能。
5. 內建四個SAM 卡

軟體設計目標為

1. 整合密碼輸入，磁條卡讀取，以及 Smart Card 讀寫介面
2. 相容於前代產品指令集，並且加入 Triple DES加密能力
3. 新增 ANSI X9.19標準之訊息認證碼產生功能
4. 強化軟體程式之強固性：將使用者功能，加密功能，硬體控制功能分層負責。
5. 強化軟體程式之安全性：儲存於記憶體中之機密資料加以安全防護

附加功能

1. 搭配磁卡讀頭模組（磁卡讀頭與本公司之 F2F 解碼 IC 組裝），可大幅簡化整體電路之設計

■執行成果

此金融應用個人密碼辨識器符合

1. Read/write ISO7816 smart cards
2. Read ISO7811/AAMVA magnetic stripe cards
3. IC Card firmware upgradeable
4. Meet DUKPT. Master/Session, MAC
5. Meet VISA PED requirement
6. Meet EMV requirement（因認證及測試費用可高達USD20,000，待客戶有需求時再做正式承認）

預計取得認證

1. EMV LEVEL 1 Compliance
2. CE、FCC Class A 及 BSMI認證

預計獲得訂單有下列廠商

1. IBM (International Business Machine Corp.)
2. NCR (National Cash Register Company)

■新產品／新技術／新設計／新材料簡介

1. 多機一體，整合磁卡（三軌）與智慧卡（T=0、T=1）讀卡功能
2. 資料防竊感應裝置當機殼被拆卸時或入侵監測電路被觸發時以下述動作之一回應：
   - 當電源被移走後記憶體歸零。
   - 入侵監測電路在數納秒內擦除內部記憶體和密鑰。
3. LCD(2x16 字元)提供完整顯示交易訊息
4. 人體工學16 鍵橡皮鍵盤 3組可程式化功能鍵，可依需求設定 Hot Key 使用
5. 支援 DES/TDES加密運算(符合 ANSI X9.8)，以及 MK/SK、DUKPT鑰匙管理設計，提供最大的安全性

PP690

PP690-combine

6. 訊息授權碼(MAC)技術，避免交易資料在傳送過程中因意外或刻意被竄改
7. 相容 VISA PED 規格，遵守 ANSI 和ISO 標準
8. 延伸相容指令：自動偵測加密鍵值長度來切換使用 DES/TDES 加密方式
9. 兩組 DUKPT 鍵值：可供客戶在不必召回機器的狀況下直接更換 DUKPT起始鍵，或從 DES 運作升級至 TDES 運作。

■技術合作單位及合作內容：無

■成果應用領域

近年來由於金融卡、信用卡偽卡猖獗，國際主要發卡組織：VISA, MASTER 及 EUROPAY共同制定了 EMV 標準以作為信用卡交易安全的新規範，國內將於 2004 年起開始全面更換符合 EMV 標準的信用卡及讀卡機，在 2008年將完成 90% 的轉換 (Card Technology, Vol.7, No.14, Dec 2002)，在歐洲 2005 年一月前將有 75% 的信用卡及 90% 的讀卡設備符合 EMV 標準 (Card Technology, Vol.7, No.11, Oct. 2002)，所以不論國內外，EMV 的規格推行將使內建IC卡的個人密碼辨識器成為交易櫃檯不可或缺的設備。連宇公司延續在磁卡讀寫卡設備十餘年的經驗，近年來投入 IC 卡讀寫卡設備的研發及生產製造。本案所開發之“金融應用個人密碼辨識器”是將連宇公司的技術能力、既有產品及市場需求作一整合和提昇。

除了以上所列之信用卡及金融卡應用外，該金融應用個人密碼辨識器之衍生機種尚可以應用於：

衍生性產品：

- 金融交易
  - 個人密碼安全模組 (Security Module)
  - Kiosk 交易模組 (Payment Module for Kiosk)
  - 自動販賣機交易模組 (Payment Module for Vending Machine)
  - ATM個人密碼安全模組 (ATM PIN Security Module)
- 應用範圍
  - 金融卡資料讀取及個人密碼輸入之處理
  - 識別卡資料讀取及個人密碼輸入之處理
  - 信用卡資料讀取及個人密碼輸入之處理

在“金融應用個人密碼辨識器”中，主要的進口關鍵技術是個人密碼資料的加解密技術，該技術之應用除了本案的個人密碼辨識器外，更可以運用於一般資料的加解密用途，提昇資訊時代資料傳遞之安全性。

跟據世界市場及國內市場現況， IC晶片卡的應用領域將持續成長擴大，配合連宇公司完整的全球行銷體系，必將為本產品創造可預期的銷售量及業績。

■專案執行績效說明

預估收益

- 首年約5000 台，營業收入 NT$17,500,000，利潤NT$4,970,000
- 第二年10000台，營業收入 NT$35,000,000，利潤NT$9,940,000
- 第三年20000台，營業收入 NT$70,000,000，利潤NT$19,880,000

- 依各個需求為客戶、專案得量身訂製、修改該產品規格以符合客戶之系統，建立了不易被取代之專案供應商
- 在該產品推展之餘，除了建立專案供應商關係外更能藉此爭取 OEM 、 ODM等 contract manufacture之機會

■專案執行重要心得

無論是護照 /身份驗證設備，或者是便利店內的銷售點終端，都有一些重要資訊，例如個人身份識別號(PIN)、密鑰和專有加密演算法等，需要特別保護以防失竊。金融服務領域採用了各種精細的策略和程式來保護硬體和軟體。因此，對於金融交易系統的設計者來講，在設計一個每年要處理數十億美元業務的設備時，必將面臨嚴峻挑戰。

為確保可信度，一個支付系統必須具有端到端的安全性。為了實現真正的安全性，本公司新開發的“金融應用個人密碼辨識器”建立在安全的硬體保護機制上，並使用可以信賴的運算內核。這樣，執行運算的晶片在發生入侵事件時就可以迅速刪除密鑰和資料記憶體，實現對資料安全的保護，對於安全資訊來講就增加了一道保護屏障。安全微控制器最有效的防護措施就是，在發現入侵時迅速擦除記憶體內容。

在“金融應用個人密碼辨識器”上，連宇公司整合了幾項重要功能：如支援 DES/TDES 加密運算(符合 ANSI X9.8)，以及 MK/SK 、 DUKPT鑰匙管理設計，提供最大的安全性，而且連宇更將自行研發之 F2F 解碼 IC 整合在此模組上，在應用產品中可提供降低成本、小空間的優點。

對於科技新興發展的今天，各種保密防竊的技術也不斷推陳出新，面對大量的信用卡側錄、盜刷，證照偽造事件，單純的紙張印刷證照及磁條卡片，已不能滿足安全防偽和資料量增多的需求。而本公司新開發的“金融應用個人密碼辨識器”以安全而且可靠的方式來取得使用者的「個人認證號碼」(Personal Identification Number - PIN)。它會以互動的方式指示或是回應使用者的動作。而使用者所輸入的 PIN 將會利用本公司自行開發依據業界標準的 DES/TDES 法則加密後，才傳回主機，最適合用於 ATM, Kiosks 等設備。況且晶片卡的時代已經來臨了，而IC晶片卡強大的安全機制及大量的儲存空間恰好能滿足這方面的需求。本開發案主要特色在於針對資訊的產生、存取、使用、和傳輸之每一流程提供層層且完整的防護保全措施，機殼也附有感應裝置，在遭受有預謀的竊賊者入侵時會自動清除記憶體內資料，防止歹徒竊取資料，提供最完整的安全機制及防護。

連宇公司延續在磁卡讀寫卡設備十餘年的經驗，近年來投入 IC 卡讀寫卡設備的研發及生產製造。本案開發之“金融應用個人密碼辨識器”是將連宇公司的技術能力、既有產品及市場需求作一整合和提昇。

本案並搭配磁卡讀頭模組（磁卡讀頭 PCB 板上，使用者只需將解碼後的 bit-幅簡化整體電路設計）之開發設計，提供與本公司之 F2F 解碼 IC 組裝於最小尺寸之 string 資料再加以轉換使用及可，如此可以大時程及材料成本）的機會，相信更能增加使用者更多選擇及降低成本（縮短設計開發產品競爭力，降低開發風險。

PP690- 正面