ISO7816 (Smart Card) 量測技術大觀

ISO7816介紹

國際標準ISO7816規範了Smart Card 規格，ISO7816文件規範說明如下:

● ISO7816-1 (Physical characteristics) :

定義物理層規範，包含Smart Card可承受工作溫度、靜電耐受度或可承受彎曲及重量等等，此一部分對於卡片製造商而言比較重要，有助於製造商選擇卡片製造材料。

● ISO7816-2 (Dimensions and location of the contacts) :

定義尺寸及連接器，包含卡片上的接腳位置及Smart Card尺寸。

● ISO7816-3 (Electrical interface and transmission protocols) :

定義電氣訊號及通訊傳輸協定。

● ISO7816-4 (Organization security and commands for interchange) :

From Abstract of www.iso.org

定義了在卡片中如何使用application identifier檢查是否存在or/and狀態的應用檢索：

- 連接介面上的命令交換回應
- 表示卡片上的retrieval of data elements 及data objects
- 表示卡片中的應用及資料結構
- 表示卡片中的identifying 及addressing applications 結構
- 描述卡片的工作特徵的歷史字節結構和內容
- 卡片中的檔案及資料存取方式
- 卡片中傳輸存取演算法
- 在卡片中對於檔案及資料保密結構
- 加密傳輸方式

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36134

● ISO7816-5 (Registration of application providers) :

From Abstract of www.iso.org

表示如何通過國際認可授權規範以及相關定義。

具有以下的功能：

・ 註冊方式

・ 相關負責機構

・ 描述註冊相關程序及應用部分

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34259

● ISO7816-6 (Interindustry data elements for interchange) :

From Abstract of www.iso.org

2004年指定Data Elements (DEs)做為數據元素根據集成電路卡片(ICCs)。 定義了DE標識符號、名稱、描述、格式、編制程序和layout並定義了DEs檢查卡片的方式。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38780

● ISO1816-7 (Interindustry commands for Structured Card Query Language) :

Structured Card Query Language (SCQL) 中的Interindustry commands說明。

● ISO7816-8 (commands for security operations) :

From Abstract of www.iso.org

2004 年定義了智慧卡中interindustry 命令(包含接觸式及非接觸式) 可用於cryptographic operations。這些命令定義是基於ISO/IEC 7816-4中的命令列表。

附錄部分提供了數位簽章範例、certificates and the import 及export of asymmetric keys。

對密碼機制的用途的選擇和條件也許影響卡片exportability，運算法及匯流排內容則不屬於ISO/IEC 7816-8內容。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37989

● ISO7816-9 (Commands for card management) :

From Abstract of www.iso.org

定義了智慧卡中interindustry命令（包含接觸式及非接觸式）的檔案管理，如檔案新增或刪除等。這些命令包含了卡片中entire life cycle及其他發佈使用時的命令。

附錄的部份則是提供如何控制讀取（保密傳輸）卡片上的資料，意指在加密狀況下傳送及驗證資料，如code、 keys及applets。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37990

● ISO7816-10 (Electronic signals and answer to reset for synchronous cards) :

From Abstract of www.iso.org

這章節定義了智慧卡從介面到裝置同步傳輸時的電源、訊號以及重置結構。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30558

● ISO7816-11 (Personal verification through biometric methods) :

From Abstract of www.iso.org

這章節定義了在智慧卡中關於personal verification through biometric methods的interindustry commands與data objects使用方式。

interindustry commands定義請參閱ISO/IEC 7816-4. data objects 國際標準化定義請參閱ISO/IEC 19785-1。

ISO/IEC 7816-11 也提供了關於註冊、驗證及位址保密的範例。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31419

● ISO7816-12 (USB electrical interface and operating procedures) :

From Abstract of www.iso.org

這章節定義了智慧卡在USB介面中的操作條件，一張使用USB介面的智慧卡稱為USB-ICC

ISO/IEC 7816-12 : 2005年定義了下列部分：

- USB-ICC電氣特性條件，當USB-ICC以介面方式進行操作。
- 標準USB描述以及USB-ICC等級描述。
- 在HOST及USB-ICC之間傳輸資料時，關於巨量傳輸及控制傳輸說明。
- 進行控制傳輸時允許兩種不同的匯流排版本。
- 表示非同步狀態下的中斷傳輸狀態以及錯誤條件。

ISO/IEC 7816-12 : 2005年針對控制傳輸提供了兩種協議版本，一種為支援protocol T=0 (version A)，另一種為transfer on APDU level (version B)。

本章節也為USB-ICC中各種傳輸提供說明圖表(巨量傳輸，控制傳輸，version A和version B)。USB-ICC一定能處理可能的序列的舉例子在情報附錄。

ISO/IEC 7816-12 : 2005年為控制轉移提供二個協議。這是為了支持協議T=0（版本A)或在APDU水平(版本B)上使用調動。USB-ICC提供說明圖表為每一調動(批量轉移，控制轉移版本A和版本B)。附錄中提供了USB-ICC範例。

Link form http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40604

● ISO7816-13 (Commands for application management in multi-application environment) :

本文介紹在開發Global Platform 標準相關事項，例如安全通道協議。

● ISO7816-15 (Cryptographic information application) :

From Abstract of www.iso.org

定義智慧卡應用。關於密碼功能的應用。2004年定義了針對密碼訊息和共享機制的共同的語法(在ASN.1)和格式。

ISO/IEC 7816-15 : 2004年支援以下功能:

- 在智慧卡中儲存多組密碼。
- 使用密碼訊息
- Retrieval密碼訊息
- DOs在ISO/IEC 7816定義了最適當的Cross參考密碼信息
- Different認證機構
- Multiple密碼算法
- Cross-referencing of the cryptographic information with DOs defined in ISO/IEC 7816 when appropriate.

ISO7816-1 ~ ISO7816-13, ISO7816-15定義了Smart Card各種規格，接著將介紹Smart Card以及如何進行測量。

Smart Card介紹

Smart Card中文名稱為智慧卡，或稱為積體電路卡(Integrate Circuit Card)，是由法國人Ro-land morono 於1974年發明，將具有儲存資料及加密保護功能的電路晶片封裝於跟信用卡大小一樣的塑膠卡片中，這樣子便成了常見的 Smart Card，法國BULL公司於1976年首先製成產品並開始應用於各種領域之中。

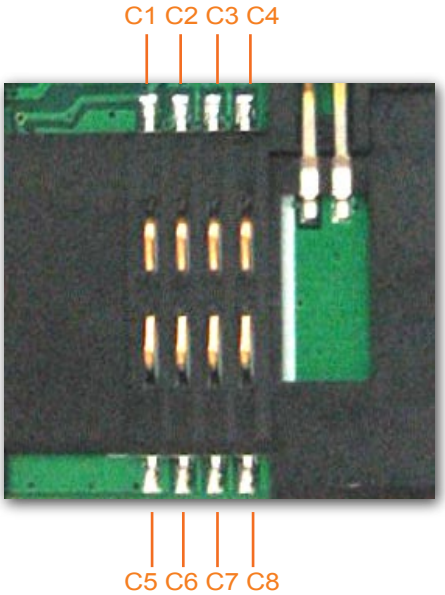
目前常見的Smart Card應用有手機內的sim卡、銀行金融卡、信用卡以及捷運悠遊卡等。

▶ 圖一：市面上常見的Smart Card 種類

“表一”為Smart Card接腳敘述，“圖二”為一般市售Smart Card Reader插槽，透過實體圖片標示更能清楚了解各腳位位置標示。

Contact	Designation	Use
C1	Vcc	Power connection through which operating power is supplied to the microprocessor chip in the card.
C2	RST	Reset line through which the IFD can signal to the smart card’s microprocessor chip to initiate its reset sequence of instructions.
C3	CLK	Clock signal line t hrough which a clock signal can be provided to the microprocessor chip. This line controls the operation speed and provides a common framework for data communication be-tween the IFD and the ICC.
C4	RFU	Reserved for future use
C5	GND	Ground line providing common electrical ground between the IFD and the ICC.
C6	Vpp	Programming power connection used to program EEPROM of first generation ICCs.
C7	I/O	Input/output line that provides a half-duplex communication chan-nel between the reader and the smart card .
C8	RFU	Reserved for future use.

▶ 表一：Smart Card 腳位敘述

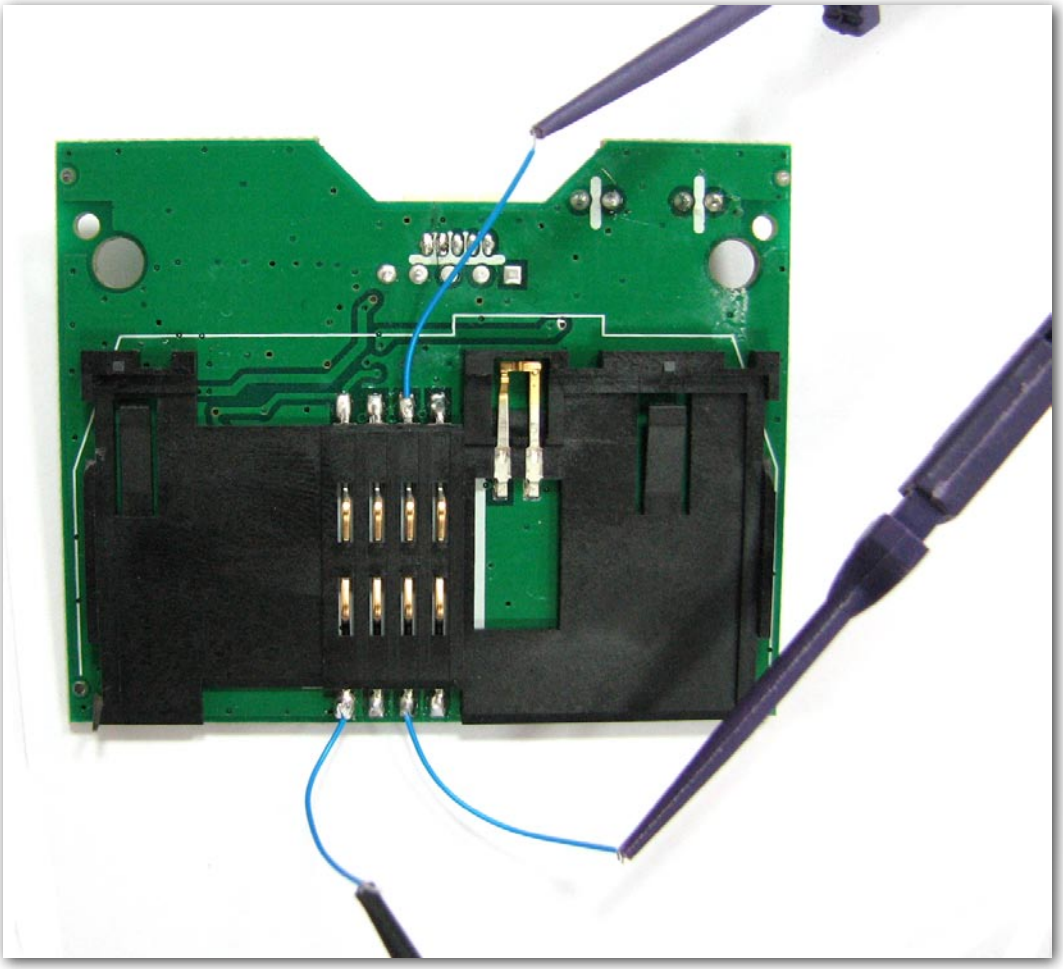


▶ 圖二：Smart Card Reader 腳位標示

使用孕龍邏輯分析儀進行ISO7816實際訊號測量

Smart Card上共有八支腳位，進行訊號測量時僅需將C3、C5、C7接至孕龍邏輯分析儀上。

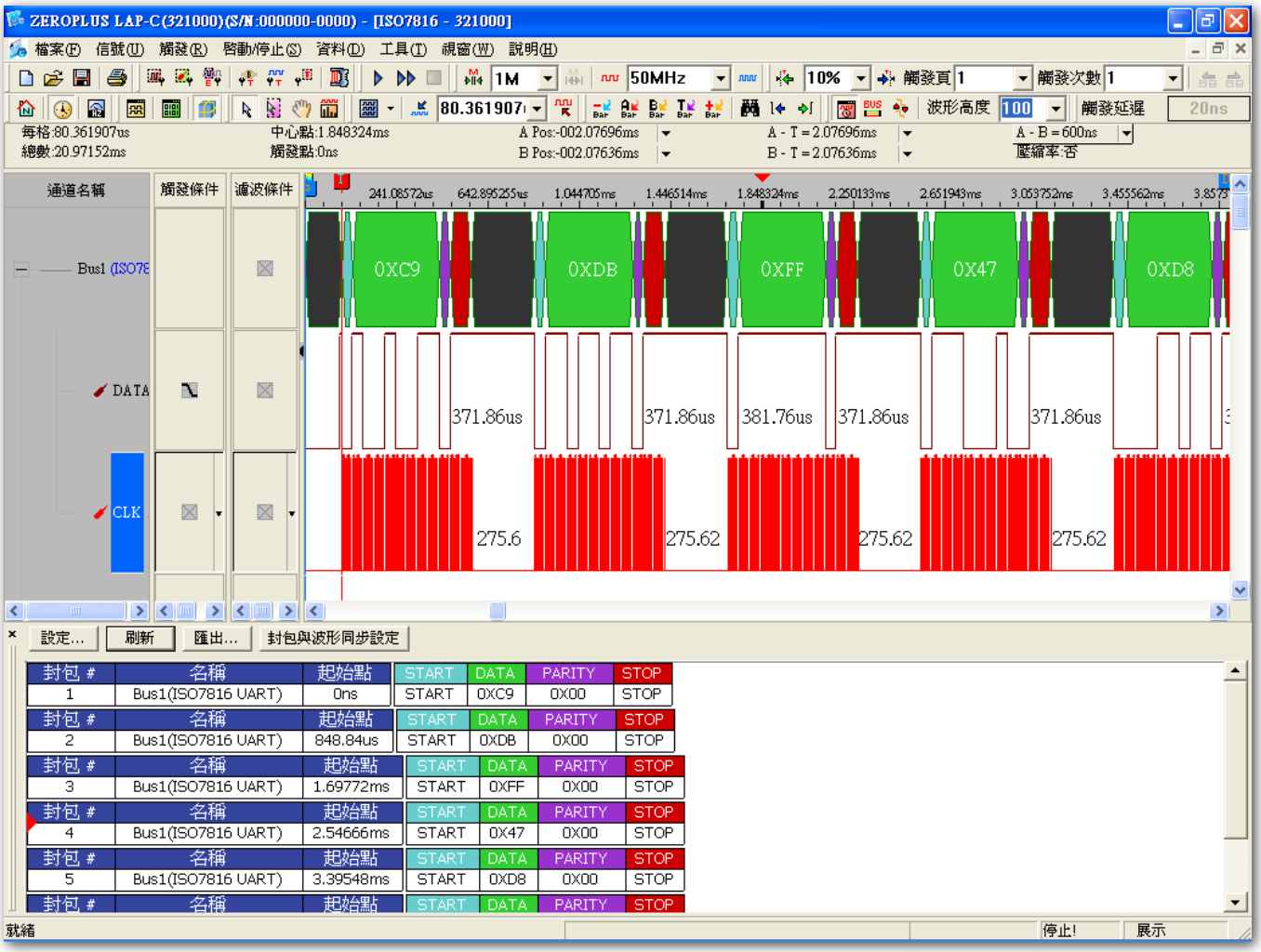
C3	CLK	Clock signal line
C5	GND	Ground line
C7	I/O	Input/output line



▶ 圖三：測量Smart Card Reader

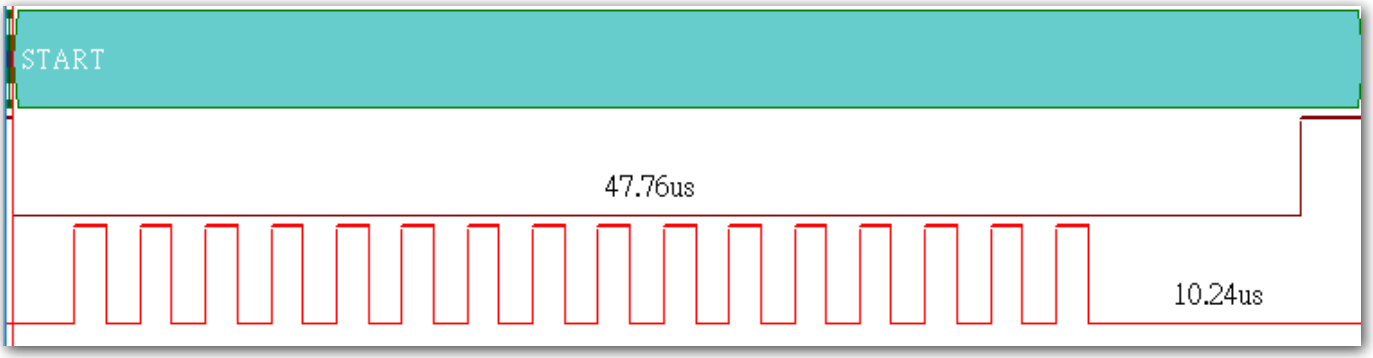
透過孕龍邏輯分析儀測試鉤可接測試點接出至邏輯分析儀上。接著分別將C3接至邏輯分析儀通道A0、C7接至邏輯分析儀通道A1、C5則接至邏輯分析儀GND上。

連接完成後便可以開啟孕龍邏輯分析儀軟體進行訊號測量（邏輯分析儀操作方式請參閱孕龍科技網站www.zeroplus.com.tw），擷取完成波形如“圖四”所示。



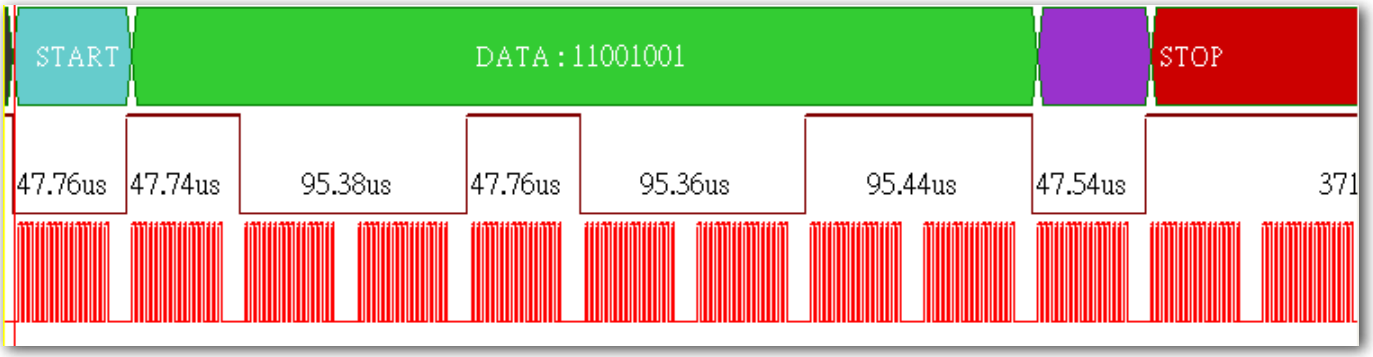
▶ 圖四：擷取完成畫面

ISO7816訊號架構上類似RS-232C方式，差異的地方在於ISO7816判斷資料需仰賴CLOCK，而RS-232C則是以自身訊號中的Baud rate，ISO7816以CLOCK 16bit 為一單位進行Data取樣，如“圖五”所示。



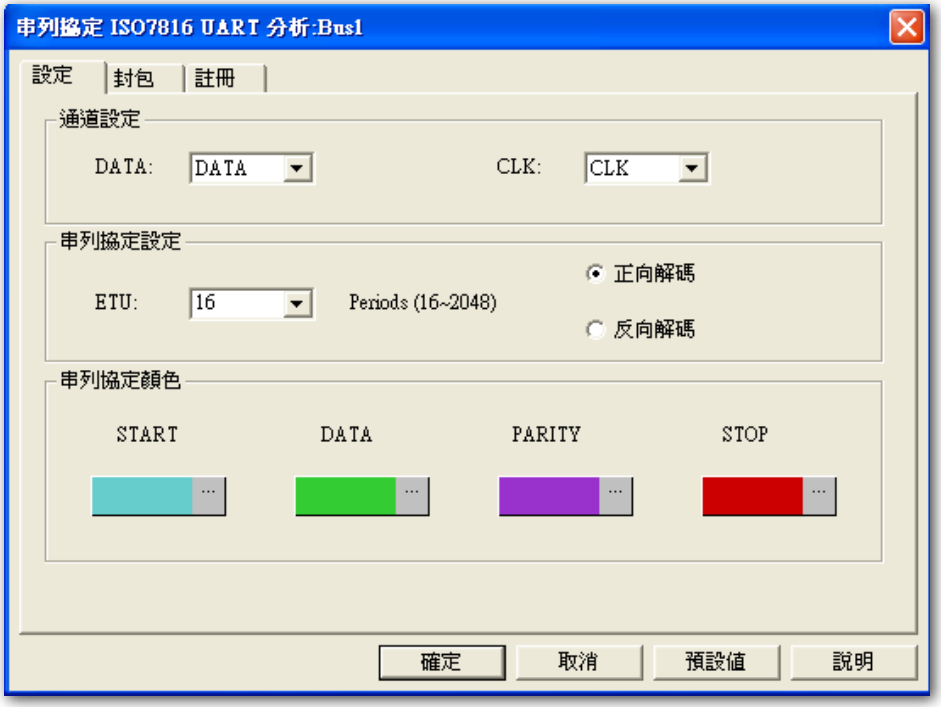
▶ 圖五：ISO7816 Start 封包

透過“圖五”可看見，START bit下方CLOCK需震盪16次後才做判斷(ETU)，以同樣的方式接著分析DATA封包的部份。



▶ 圖六：完整 ISO7816 訊號封包

訊號封包格式由START (1bit) + DATA (8bits) + PARITY CHECK (1bit) + STOP (2bits)組成，DATA線上每一個bit都需滿足CLOCK線上出現16次震盪 (ETU)，而DATA傳輸方向固定為LSB to MSB。



▶ 圖七：孕龍邏輯分析儀ISO7816匯流排模組介面

通道設定：可設定DATA及CLK通道位置

串列協定設定：可設定ISO7816訊號中1bit判斷的震盪長度，預設值為16，最高可設定至2048

總　結

Smart Card (ISO7816) 的應用十分廣泛，從金融卡、手機SIM卡到捷運悠遊卡都是使用ISO7816進行訊號傳輸，近年來更因為網路ATM轉帳需求而出現USB介面的ATM讀卡機，各式各樣的應用商品問世，使得個人生活越來越便利，這些都是因為科技數位化蓬勃發展導致，但這也正考驗者產品研發設計的工程師們，如何在第一時間提供更方便的產品，該如何順利完成產品設計專案讓產品上市就是首要考慮的問題。

孕龍科技邏輯分析儀推出了五十多種匯流排解碼模組，針對研發工程師在分析匯流排訊號時，可透過軟體自動解碼功能縮短開發專案的時間，及早讓商品問世，面對各種數位訊號時不需要再透過示波器進行手動解碼方式來分析訊號。
關於更多孕龍邏輯分析儀介紹請至孕龍科技網站 www.zeroplus.com.tw

參考資料:

- CardWerk form http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx
- Wikipedia ISO/IEC 7816 form http://en.wikipedia.org/wiki/ISO_7816