SmartCard Reader Athena

Melvin Gutierrez *,Oscar Montes†, Michael Varela‡ Área de Ingeniería en Computadores, ITCR
Email: *melving@estudiantec.cr, †oscarm@estudiantec.cr, ‡michaelv@estudiantec.cr

***Abstract*—Este artículo, pretende mostrar el funcionamiento de un *SmartCard Reader Athena*, los cuales son un dispositivo que es provisto cuando se adquiere una Firma Digital en Costa Rica. En la descripción se trata de abarcar tanto características del protocolo de comunicación del lector con la SmartCard Athena IDProtect Duo con LASER PKI, así como la interacción de los bloques principales del dispositivo lector para permitir el correcto funcionamiento.**

***Keywords*—Athena, Applet, SmartCard Reader.**

I. Introducción

ANTES de iniciar con las características propias de la Smart Card Reader,es importante conocer el concepto de firma digital,ya que este es un método que asocia la identidad de una persona o equipo, con un mensaje o documento electrónico, para asegurar la autoría y la integridad del mismo. La firma digital del documento es el resultado de aplicar algoritmos matemáticos a su contenido que crean una secuencia que únicamente puede haber sido creada por el poseedor del certificado digital[1].
Las tarjetas que hacen uso de la firma digital en Costa Rica utilizan la SmartCard Athena IDProtect Duo con LASER PKI la cual utiliza el estandar *ISO/IEC 7816* y el ISO 14443 [2] debido a este motivo, se pretende mostrar en la siguiente sección características generales del estándar, luego como las tarjetas son leídas siguiendo este estándar utilizando un módulo genérico, ya que el SmartReadear de Athena *ASEDrive IIIe USB V3/V3C* no provee los diagramas de circuito que demuestran el proceso completo de la comunicación. Siguiente a esta sección se presentan algunas características del intercambio de paquetes y por ultimo se presentan las conclusiones de la investigación.

II. Descripción del Estándar

Para mostrar el funcionamiento de la SmartCard Reader de Athena, se pretende describir las principales partes del estándar ISO 7816, para mostrar el proceso de lectura de las tarjetas.
El estándar actualmente con 15 partes (o niveles), pero sólo algunos de ellos son relevantes para propósitos de esta investigación[3].

A. Contactos Tarjeta

La siguiente tabla contiene la definición de contacto de los contactos eléctricos, según ISO7816-2:, las terminales indicadas en la "Tabla 1", corresponden a los contactos de la tarjeta presentados en la "Figura 1"

TABLE I. Conexiones Eléctricas SmartCard

Contacto	Designación	Uso
C1	Vcc	Es la conexión de energía que provee el lector hacia el microprocesador que se encuentra en la tarjeta, usualmente son 5V, con 200mA como máximo. Sin embargo, hay otros de 3.3V.
C2	RST	Linea de reset,(desde el lector hacia la tarjeta).
C3	CLK	Señal de clock, (desde el lector hacia la tarjeta).
C4	RFU	Reservado para uso futuro.
C5	GND	Tierra común entre el lector y la tarjeta.
C6	Vpp	Alto voltaje utilizado para programar la EEPROM en chips antiguos.
C7	I/O	Linea de datos I/O que provee una comunicación half-duplex entre el lector y la tarjeta.
C8	RFU	Reservado para uso futuro

Fig. 1. Conexiones Físicas SmartCard

III. Señal Eléctrica y Protocolo de Transmisión

La comunicación con la tarjeta inteligente se lleva a cabo a través de una sola línea de datos bidireccional, half-duplex. Los niveles de tensión para los estados de alta / baja es la misma que la tensión de alimentación a la tarjeta inteligente.La dirección de la comunicación se supone que es conocido a priori tanto por el maestro (lector) y el esclavo (tarjeta inteligente). Parámetros como formato de protocolo, tipo de tarjeta inteligente, la velocidad de transmisión y otros parámetros eléctricos se leen de la tarjeta inteligente después de reinicio.Esto se conoce como la respuesta restablecer o ATR. Con base en la información proporcionada en el ATR, el lector puede adaptarse al formato de transmisión soportado por la tarjeta.
Muchas de las implementaciones se basan en la siguiente interfaz para la comunicación, puesto que la comunicación de datos es bidireccional, el terminal es a menudo configurado

para transmitir datos a través de una salida de drenaje abierto. Esto significa que puede tirar de la baja línea de datos, pero se necesita una resistencia pull-up para ir alta de nuevo. Y de la misma manera, la tarjeta inteligente puede tirar de la línea de baja, pero necesita el pull-up para tomar la línea de alta de nuevo. Esto se ejemplifica en la "Figura 2".

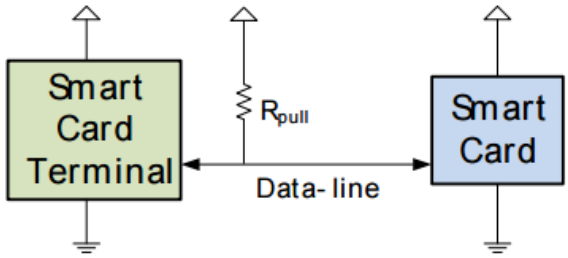

Fig. 2. Linea de datos Bidireccional con Resistencia Pull-Up

Power Up, Clock y Reset Cuando se inserta una tarjeta en el lector, todos los contactos se desconectan de la terminal / lector, incluyendo la de tierra. La razón de esto es que los contactos de la diapositiva de terminales en los contactos de la tarjeta inteligente mientras se inserta la tarjeta. La aplicación de la potencia a las patillas equivocadas en teoría, podría dañar la tarjeta o el lector.Cuando la tarjeta se ha insertado correctamente, por lo general hay un contacto eléctrico que rompe la conexión, lo que indica al lector que la tarjeta esté completamente insertada. Ahora el lector inicia una secuencia de encendido y reset.La interfaz es responsable de la temporización de la secuencia. Los parámetros más importantes son el recuento clockcycle antes y después de soltar restablecimiento.La interfaz debe permitir al reloj y que siga funcionando de 40k ciclos antes de la liberación de restablecimiento. Después de restablecimiento, la tarjeta debe responder con su ATR dentro de una ventana de 400-40000 ciclos de reloj.El diagrama de ciclos se presenta en la "Figura 3".

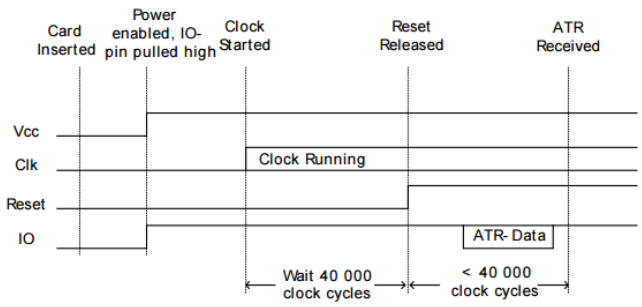

Fig. 3. Answer to Reset Sequence

Transferencia de Bytes Durante el encendido y reset secuencia de las respuestas de tarjetas inteligentes, con su "Answer to Reset".
La transmisión de este primer paquete de datos se lleva a cabo con los parámetros de comunicación por defecto se indican a continuación(Ver "Figura 4"):

- Velocidad de transmisión = FClock/372. El Clock debe ser de aproximadamente 3,57 MHz, dando lugar a 9,6 kbit/s.
- 8 data bits.
- 1 start bit.
- 1 parity bit
- 1.5 stop bits
- Codificación de 0's y de 1's.

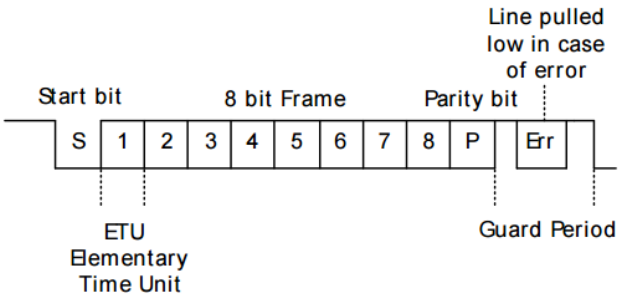

Fig. 4. Byte Transmisión, Paridad y Tiempo Unidad Elementaria

A. *Answer to Reset*

El "Answer to Reset" es una cadena de 33 o menos caracteres (bytes). Con nombrando como se define en la norma ISO 7816-3, el ATR se compone de los siguientes caracteres obligatorios y opcionales:

- TS - un carácter inicial obligatoria, transmitiendo el byte de formato, (la convención directa o inversa)
- T0 - un carácter obligatorio de formato, lo que indica el contenido de la ATR
- Tai, TBI, el TCI, TDi - caracteres de interfaz opcionales, estos caracteres indican, las velocidades soportadas reloj, niveles de tensión y protocolos soportados por la tarjeta. Puesto que son opcionales, si no se da, el lector de tarjetas debe continuar con el protocolo predeterminado que se utiliza durante la secuencia ATR.
- T1, T2, TK - caracteres históricos opcionales, estos caracteres suelen tener información sobre la tarjeta fabricante, tipo de tarjeta (tamaño, etc.), número de versión y el estado de la tarjeta.
- TCK - un carácter de control condicional, la presencia de este byte se indica con los caracteres de interfaz opcionales, si está presente, es O exclusivo de todos los bytes en el ATR, con exclusión de TS y TCK.

IV. Comandos e intercambio de paquetes de datos

El canal es un medio-duplex, canal físico. Parte 4 de la norma ISO 7816 define los protocolos de nivel de enlace en la parte superior de este canal físico. El protocolo de nivel de enlace proporciona un canal de comunicación libre de error

para el protocolo de nivel de aplicación. En esta sección se describe la estructura del mensaje que consta de unidades de datos de protocolo de aplicación (APDU), que se intercambian entre la aplicación de lector y de la aplicación de tarjeta inteligente por el protocolo de nivel de enlace.
Parte 4 de la norma 7816 también define una API del sistema de archivos para manipular archivos y una API de servicio de seguridad que permite la tarjeta inteligente y el lector para autenticar mutuamente entre sí[3].

A. *Unidades de Datos del Protocolo*

Las unidades de datos transmitidos en el protocolo de capa de enlace se denominan unidades de datos de protocolo de transmisión (TPDU). Estos son los paquetes de datos que van entre el lector y la tarjeta inteligente. En la parte superior de estos son la APDU, que viene directamente de la capa de aplicación del protocolo. Las APDU se transmiten normalmente inalterado por el dispositivo de interfaz de tarjeta inteligente, pero esto depende del nivel de automatismo apoyado por el lector. A continuación se muestra un esquema que muestra el diagrama general("Figura 5").

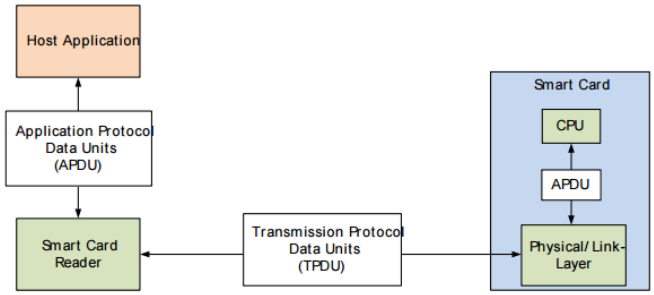

Fig. 5. Unidades y datos de protocolo donde se aplican

V. Conclusiones

La seguridad hoy por hoy tiene un papel muy importante en gran variedad de áreas es por eso las SmartCards juegan un papel muy importante por su bajo costo y seguridad robusta. En esta investigación lo encontrado de mayor relevancia es que al poseer un protocolo común, diferentes tarjetas de diferentes fabricantes operan de una forma similar, por lo que siguiendo el protocolo se puede aplicar ingeniería inversa a la tarjeta que se desea leer y así poder construir un lector que pueda leer correctamente las mismas,

References

[1] "¿Qué es Firma Digital?" [Online]. Available: https://www.soportefirmadigital.com/web/es/que-es-firma-digital.html#ms-sobre-como-se-firma-digitalmente-un-documento

[2] Banco Central Costa Rica, "E S T Á N D A R F Í S I C O F I R M A D I G I T A L SERIE DE NORMAS Y PROCEDIMIENTOS," 2015. [Online]. Available: http://www.bccr.fi.cr/normas_sinpe/EstandarFisicoFirmaDigital.pdf

[3] silabs, "EFM32 USB Smart Card Reader." [Online]. Available: http://www.silabs.com/Support%20Documents/TechnicalDocs/AN0820.pdf