คำแนะนำการพัฒนาโปรแกรมอ่านบัตร Mifare สำหรับ Feitian RFID Reader

R&D Computer System Co., Ltd.

ส่วนประกอบซอฟต์แวร์ชุดพัฒนา

- Documents
  - เป็นที่เก็บของไฟล์เอกสารทั้งหมด ได้แก่
    - Datasheet ของชิป เช่น Mifare
    - คำสั่ง APDU ของเครื่องอ่าน
- Drivers
  - ไดรเวอร์ สำหรับ Windows XP
- SourceCode
  - ตัวอย่างโปรแกรม เพื่อการอ่านบัตร RFID
- Utilities
  - เครื่องมือสำหรับใช้ในการทดสอบ
- Guideline
  - แนวทางการพัฒนา พร้อมเอกสารและโปรแกรมที่จำเป็นสำหรับการพัฒนา

เครื่องอ่านบัตร RFID ของ Feitian ที่รองรับ

- R502-Dual
- R502-CL

บัตร Mifare

โครงสร้างข้อมูลของบัตร Mifare ขนาด 1 KByte มีดังนี้

- บัตรจะแบ่งข้อมูลออกเป็นเซ็คเตอร์ (Sector) ทั้งหมด 16 เซ็คเตอร์ (ตั้งแต่ 0 ถึง 15) ในแต่ละเซ็คเตอร์ประกอบ ด้วยชุดข้อมูล 4 บล็อก (Block) รวมเป็น 64 บล็อก (เรียก Block 00-63) โดย 1 บล็อก จะมีข้อมูล 16 ไบต์
- Block 0-2 ของแต่ละเซ็กเตอร์ เป็นพื้นที่เก็บข้อมูล สามารถเขียนอ่านได้
- Block 3 ของแต่ละเซ็กเตอร์ เป็นพื้นที่เก็บกุญแจรหัสในอ่านเขียนข้อมูลของบล็อกนั้น ปกติไม่ได้ใช้เก็บข้อมูล แต่จะใช้เก็บรหัสกุญแจและตาราง Access Bits
  - Byte 0-5 เก็บรหัส Key A
  - Byte 6-9 เก็บตาราง Access Bits
  - Byte 10-15 เก็บรหัส Key B
- เฉพาะ Block 0 ของ Sector 0 จะเก็บข้อมูลพิเศษของผู้ผลิต เช่น UID อ่านได้อย่างเดียว เขียนทับไม่ได้
- การควบคุมการเข้าถึงหน่วยความจำ

- ต้องใช้รหัสกุญแจในการอ่านหรือเขียน เป็นการควบคุมระดับเซ็กเตอร์
- พื้นที่หน่วยความจำของทุกบล็อกในเซ็กเตอร์เดียวกัน จะใช้รหัสกุญแจชุดเดียวกัน
- ข้อมูลแต่ละเซ็กเตอร์ สามารถมีกุญแจควบคุมได้ 2 ตัว คือ Key A กับ Key B
- ข้อมูลแต่ละบล็อกสามารถใช้กุญแจ Key A หรือ Key B ในการอ่านหรือเขียนก็ได้

- รายละเอียดศึกษาได้จากคู่มือของชิป Mifare (เป็นไฟล์อยู่ในชุดพัฒนา)

ขั้นตอนการอ่านเขียนบัตร Mifare

- เชื่อมต่อกับบัตร
- ส่งรหัสกุญแจ (Key) ให้กับบัตร
- สั่งให้ตรวจสอบรหัสกุญแจ
- สั่งอ่านหรือเขียนข้อมูลที่ต้องการ
- สั่งหยุดการเชื่อมต่อ

คำสั่ง APDU

APDU คือชุดคำสั่งในการสั่งานบัตร เครื่องอ่านและบัตรแต่ละรุ่นโดยมากจะมีคำสั่งที่เหมือนกัน แต่อาจมีคำสั่งที่แตกต่างกันบ้าง สามารถดูคำสั่งทั้งหมดอย่างละเอียดได้จากคู่มือของเครื่องอ่านแต่ละรุ่น ซึ่งเป็นไฟล์อยู่ในโฟลเดอร์ Documents ของชุดพัฒนา (สำคัญควรศึกษา)

เมื่อส่งคำสั่ง APDU ไปแล้ว บัตรจะตอบกลับมาด้วย Response อย่างน้อย 2 ไบต์ เรียกว่า SW1 กับ SW2 โดยปกติหากการทำงานถูกต้องจะได้ค่า Response เป็น 90h 00h

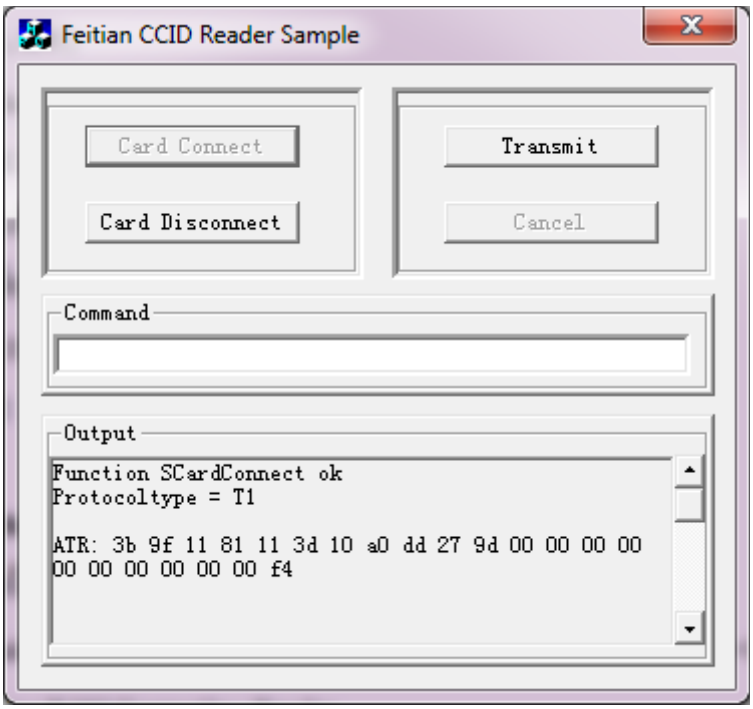
ตัวอย่างคำสั่ง APDU

- Get UID อ่านค่า UID
  - APDU : FF CA 00 00 00
  - Response : UID, SW1, SW2
- Load Keys โหลดรหัสกุญแจ
  - APDU : FF 82 00 YY 06 KK KK KK KK KK KK
    - YY คือ ตำแหน่งของ Key ปกติเป็น 00h หรือ 01h
    - KK KK KK KK KK KK คือรหัสกุญแจ 6 ไบต์ ปกติบัตรใหม่จะใช้ค่าเป็น FF FF FF FF FF FF
  - Response : SW1, SW2
- Authenticate ตรวจสอบรหัสกุญแจ
  - APDU : FF 86 00 00 05 01 00 KK TT YY
    - KK คือ หมายเลขบล็อก ที่จะอ่านหรือเขียน (00h-3Fh)

        - TT คือ Key ที่จะใช้ 60h คือ Key A 61h คือ KeyB
        - YY คือ ตำแหน่งของ Key ปกติเป็น 00h หรือ 01h
    - Response : SW1, SW2
    - หลังจาก Authenticate แล้ว จะสามารถอ่านเขียนข้อมูลในบล็อกนั้นได้ตลอด จนกว่าจะเปลี่ยนบล็อกใหม่
- Read Binary Blocks อ่านข้อมูลจากบล็อก
    - APDU : FF B0 00 KK LL
        - KK คือ หมายเลขบล็อก ที่จะอ่าน (00h-3Fh)
        - LL คือ ความยาวข้อมูลที่จะอ่าน ปกติ เป็น 10h เสมอ
    - Response : Data, SW1, SW2
- Update/Write Binary Blocks เขียนข้อมูลลงในบล็อก
    - APDU : FF D6 00 KK LL JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ
        - KK คือ หมายเลขบล็อก ที่จะอ่าน (00h-3Fh)
        - LL คือ ความยาวข้อมูลที่จะอ่าน ปกติ เป็น 10h เสมอ
        - JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ JJ คือข้อมูล 16 ไบต์ที่จะเขียน
    - Response : SW1, SW2

ตัวอย่างการทดสอบด้วยโปรแกรม ReaderSample.exe

- คำเตือน โปรดระมัดระวังในการสั่งเขียนบัตร หากเขียนลง Block ที่เก็บค่ารหัสกุญแจ (Block 3 ของทุกเซ็กเตอร์) แล้วจำค่ากุญแจไม่ได้ จะทำให้ไม่สามารถสั่ง Authenticate และอ่านเขียน เซ็กเตอร์นั้นได้อีกต่อไป
- ติดตั้งเครื่องอ่าน RFID ที่เครื่องคอมพิวเตอร์
- เรียกใช้งานโปรแกรม ReaderSample.exe (อยู่ในโฟลเดอร์ SourceCode\ReaderSample_C++\Release)
- เลือกใช้งานเครื่องอ่าน Feitian R502 Contactless Reader (โปรดสังเกตชื่อให้ดี ว่าต้องเป็น Contactless)
- นำบัตร Mifare ใหม่ ที่ยังไม่เคยใช้งานวางบนเครื่องอ่าน
- คลิกที่ปุ่ม Card Connect บนหน้าจอ จะเห็นข้อมูล ATR ในช่อง Output

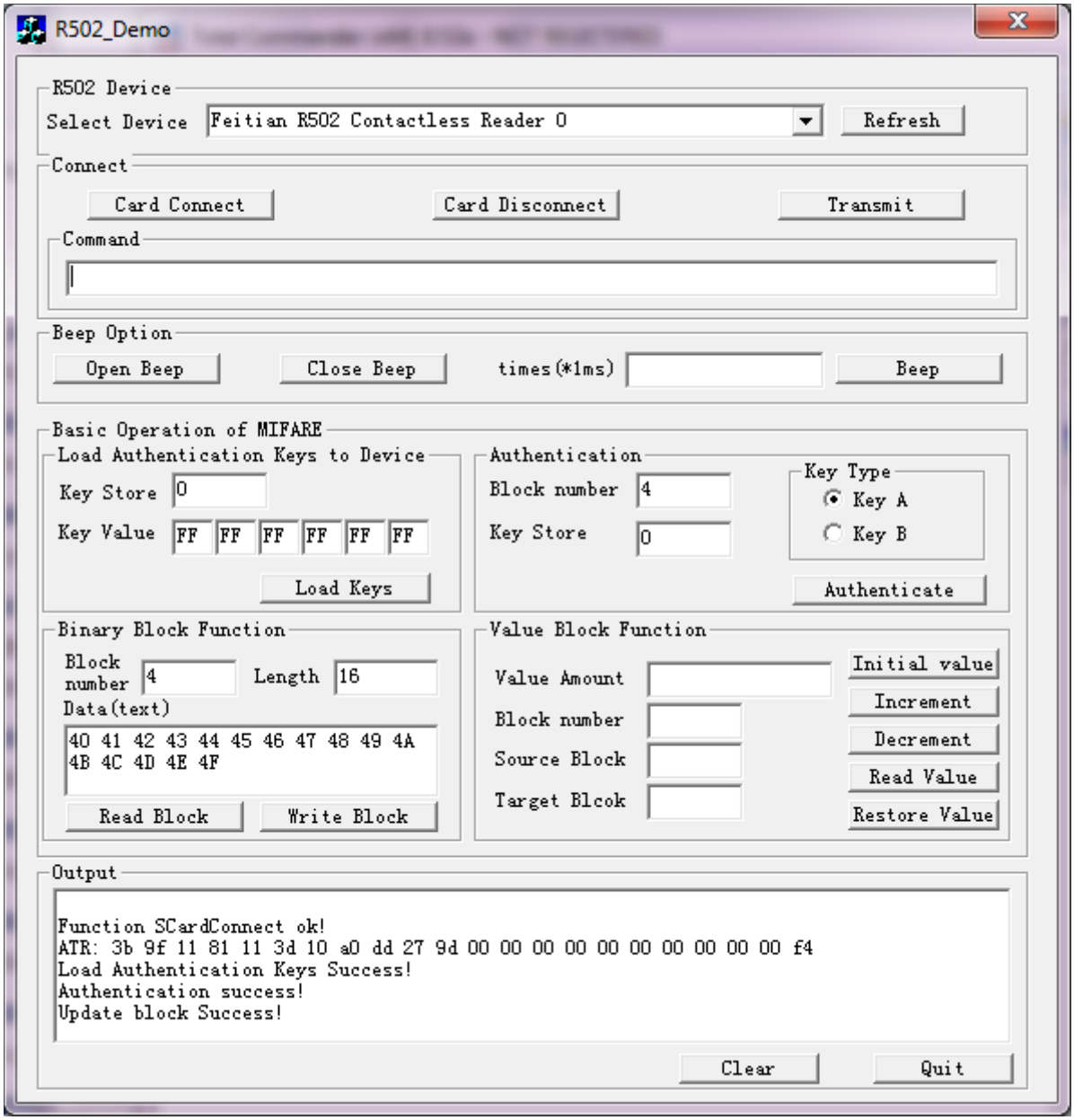


- ในช่อง Command ให้ป้อนคำสั่งแล้วคลิกที่ปุ่ม Transmit ตามขั้นตอนต่อไปนี้
  - FFCA000000 (อ่าน UID)
  - Response : XX XX XX XX 90 00 (ข้อมูล UID)
  - FF82000006FFFFFFFFFFFF (โหลดรหัสกุญแจ)
  - Response : 90 00 (ทำงานถูกต้อง)
  - FF860000050100046000 (ตรวจสอบรหัสกุญแจ ของ Block 1 ด้วย Key A)
  - Response : 90 00 (ทำงานถูกต้อง)
  - FFB0000410 (อ่านข้อมูลจาก Block 04 จำนวน 16 ไบต์)
  - Response : FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 90 00 (ข้อมูลที่อ่านได้ อาจเป็นค่าใด ๆ ก็ได้)
  - FFD6000410000102030405060708090A0B0C0D0E0F (เขียนข้อมูลลง Block 04 จำนวน 16 ไบต์)
  - Response : 90 00 (ทำงานถูกต้อง)
  - FFB0000410 (อ่านข้อมูลจาก Block 04 จำนวน 16 ไบต์)
  - Response : 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 90 00 (ข้อมูลที่อ่านได้)
- คลิกที่ปุ่ม Card Disconnect เพื่อหยุดการใช้งาน
- หมายเหตุ
  - ค่ารหัสกุญแจที่สั่งโหลด ต้องมีค่าตรงกับรหัสค่ากุญแจที่อยู่ในบัตร ปกติบัตรใหม่ที่ยังไม่เคยใช้งานจะมีค่ารหัสเป็น FF FF FF FF FF FF ส่วนบัตรที่ใช้งานแล้วหากมีการเปลี่ยนค่ารหัสกุญแจ ก็จะต้องใช้รหัสกุญแจนั้นในการโหลด
  - แหล่งศึกษาข้อมูลเพิ่มเติม

- http://pcsclite.alioth.debian.org/ccid.html
- http://pcsclite.alioth.debian.org/api/group__API.html

ตัวอย่างการทดสอบด้วยโปรแกรม R502.Demo.exe

- คำเตือน โปรดระมัดระวังในการสั่งเขียนบัตร หากเขียนลง Block ที่เก็บค่ารหัสกุญแจ (Block 3 ของทุกเซ็กเตอร์) แล้วจำค่ากุญแจไม่ได้ จะทำให้ไม่สามารถสั่ง Authenticate และอ่านเขียน เซ็กเตอร์นั้นได้อีกต่อไป
- ติดตั้งเครื่องอ่าน RFID ที่เครื่องคอมพิวเตอร์
- เรียกใช้งานโปรแกรม R502.Demo.exe (อยู่ในโฟลเดอร์ Utilities\R502Demo)
- เลือกใช้งานเครื่องอ่าน Feitian R502 Contactless Reader (โปรดสังเกตชื่อให้ดี ว่าต้องเป็น Contactless)
- นำบัตร Mifare ใหม่ ที่ยังไม่เคยใช้งานวางบนเครื่องอ่าน



- คลิกที่ปุ่ม Card Connect บนหน้าจอ จะเห็นข้อมูล ATR ในช่อง Output
- ทดลองอ่านเขียนข้อมูลตามขั้นตอนต่อไปนี้
  - ในกรอบ Basic Operation of MIFARE
    - กรอก Key Store เป็น 0
    - กรอก Key Value เป็น FF FF FF FF FF FF
    - คลิกที่ Load Keys เพื่อโหลดรหัสกุญแจ
    - ดูผลในช่อง Output ด้านล่าง
  - ในกรอบ Authentication
    - กรอก Block number เป็น 4
    - กรอก Key Store เป็น 0
    - เลือก Key Type เป็น Key A
    - คลิกที่ Authenticate เพื่อตรวจสอบรหัสกุญแจ ของ Block 04 ด้วย Key A)
    - ดูผลในช่อง Output ด้านล่าง
  - ในกรอบ Binary Block Function
    - กรอก Block number เป็น 4
    - กรอก Length เป็น 16
    - คลิกที่ Read Block อ่านข้อมูลจาก Block 04 จำนวน 16 ไบต์
    - ดูผลในช่อง Data(text)
  - ในกรอบ Binary Block Function
    - แก้ไขข้อมูลในช่อง Data(text) ทั้ง 16 ไบต์เป็นค่าที่ต้องการจะเขียน (เป็นเลขฐาน 16 ติดกันทั้งหมด)
    - คลิกที่ Write Block เพื่อเขียนข้อมูล 16 ไบต์ ลง Block 04
    - ดูผลในช่อง Data(text)
  - คลิกที่ปุ่ม Card Disconnect เพื่อหยุดการใช้งาน
- หมายเหตุ สามารถใช้โปรแกรม R502.Demo.exe นี้ส่งคำสั่ง APDU ในช่อง Command ได้เหมือนโปรแกรม ReaderSample.exe