



Advanced Card Systems Ltd.

ACR38 Software Development Kit

ACR39-SDK (CCID방식) 사용자 가이드

(주)에스씨포인트 www.scpoint.co.kr 서울시 강남구 선릉로135길 29 SH빌딩 3층
Tel : 02)515-5127, Fax : 02)515-5147 문의메일 : info@scpoint.co.kr

SDK 설치를 위한 시스템 요구사항

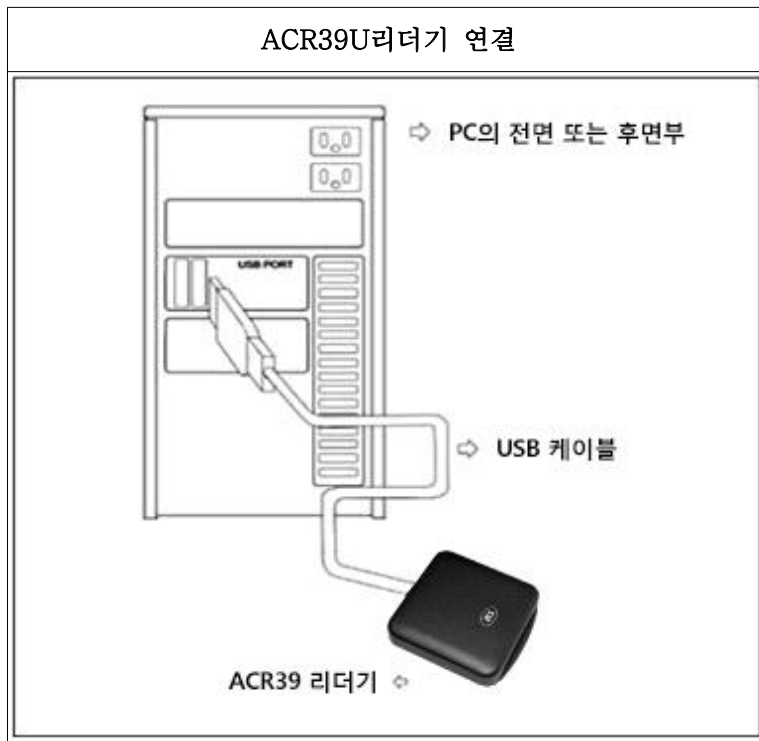
- IBM 호환 Intel Pentium 1GHz 이상의 프로세서.
- Microsoft Windows 7 / 8.1 / 10(각 64bit 포함), Linux Ubuntu
- CD-ROM 드라이브, USB port

SDK 구성품

- ACR39U IC카드 리더기 * 1개
- ACOS3 IC Card * 5장
- SLE5542 메모리형 카드 * 5장
- SLE5528 메모리형 카드 * 5장
- ACR39U SDK CD * 1장

제품 연결 구성도

※ 제품의 드라이버가 완전히 설치된 이후에 리더기를 PC에 연결시켜 주세요.



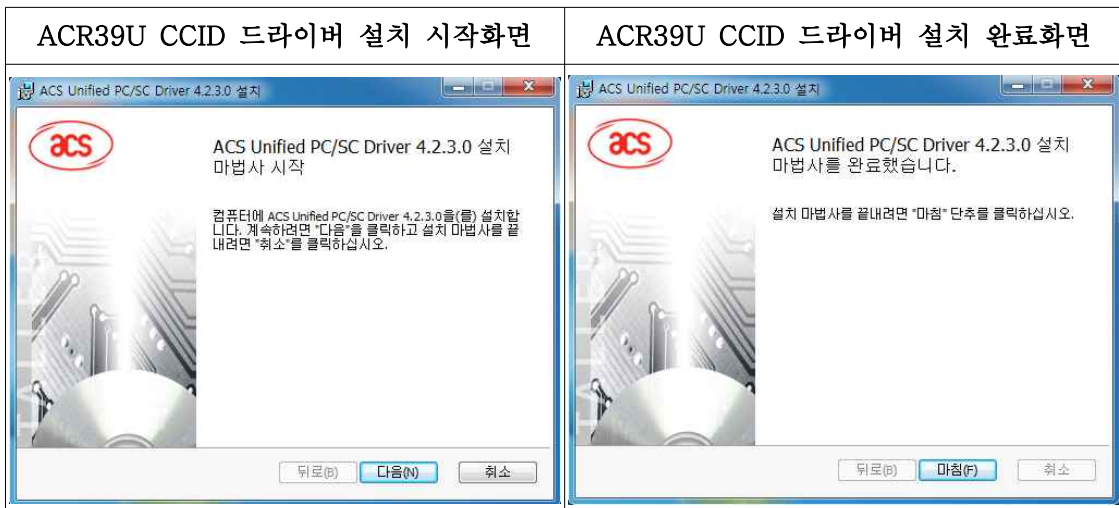
SDK 인스톨 작업

ACR39U-SDK CD를 넣거나 또는 CD-ROM이 있는 디스크명으로 이동하여 autorun.exe를 실행시키면 다음과 같은 설치화면이 나타납니다.



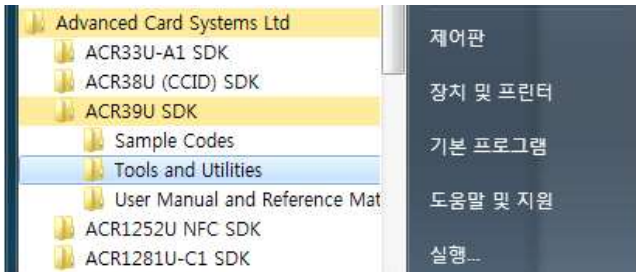
- Step 1 : 현재 보고 계신 메뉴얼의 영문판을 볼수 있습니다.
- Step 2 : ACR39U 리더기의 드라이버를 설치합니다.
- Step 3 : SDK의 구성물(language별 샘플코드, 사용자 Tool, 관련 카드 및 리더기의 PDF메뉴얼)을 설치합니다.
- Step 4 : 직접적으로 카드에 명령을 내릴 수 있는 카드 및 리더기 Tool을 설치합니다.
- Step 5 : 만약 현재PC에 Acrobat Reader가 설치되어있지 않을 경우 Step 5.를 클릭하여 제품을 설치할수 있습니다.

우선 ACR39U 리더기를 사용하기 위하여 Step 2.를 클릭하여 제품의 드라이버를 아래와 같이 설치합니다.



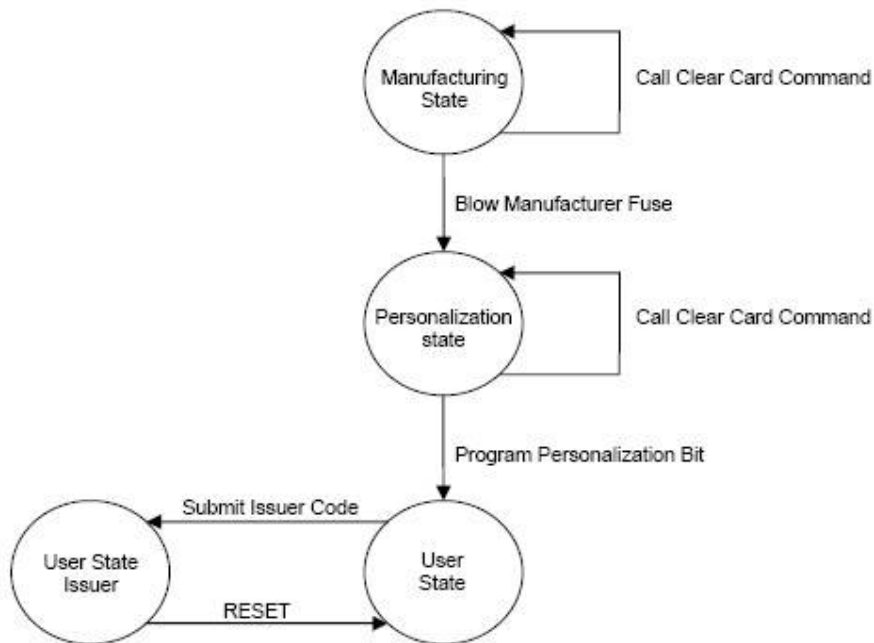
드라이버를 설치한 이후에는 Step 3.을 클릭하여 실제 어플리케이션 개발시 많은 도움이 되는 SDK 구성물을 설치합니다.

설치가 완료되면 다음과 같은 구성물이 프로그램 창에 생성된걸 확인하실 수 있습니다.



SDK 구성물 세부설명

◎ ACOS3카드 Life Cycle



1. Manufacturing 단계 : 제조 단계의 cycle로써 카드에 모든 command를 수행할수 있음.

오직 Manufacturing단계에서만 Manufacturer File(FF 01)을 write할 수 있으며 카드 제조사 식별자 번호, 카드 씨리얼번호, IC(Issuer Code)등의 값이 본 단계에서 write되어짐. 'CLEAR CARD'커맨드에 의해 카드 EEPROM내의 모든 데이터와 키값을 지울수 있으며(단, IC코드와 Manufacturer File은 삭제불가) Personalization단계로 넘어간 이후에는 다시 Manufacturing단계로 돌아올 수 없음.

2. Personalization 단계 : 개발자들이 최초 카드를 받았을때의 상태로써 User 단계로 넘어가기전의 카드세팅 작업단계. EEPROM내에 있는 각각의 Internal Date File들은 IC(Issuer Code)의 수행후에 read/write가 가능하며 'CLEAR CARD'커맨드에 의해 EEPROM

내의 데이터와 킷값을 지울 수 있음(최초 카드를 받은 상태로 초기화). User stage단계로 넘어간 이후에는 다시 Personalization 단계로 돌아올 수 없음.

엔드유저에게 카드를 배포하기 위해서는 User stage 단계에서 카드를 발급하는것이 필요하며 Personalization단계에서 User stage단계로 넘어가는 방법은 Personalization File의 첫번째 레코드의 4번째 바이트의 MSB를 '1'로 라이팅 해준후에 reset신호는 보내면 "User Stage"단계로 이동하게 됩니다.(ACOS3 Reference 메뉴얼의 8페이지 참고)

위의 내용을 자세하게 설명하면

1. Issuer Code(ACOSTEST=41 43 4F 53 54 45 53 54)를 submit합니다.
2. Personalization File(FF 02)을 select합니다.
3. Personalization File내의 00레코드의 4번째 바이트를 80으로 세팅합니다.
4. ACOS3를 reset합니다.(reset이후에 "Personalization stage"단계에서 "User Stage"단계로 넘어감)

Reset 이후에 정상적으로 세팅이되어져서 "User Stage"단계로 넘어갔다면 Reset신호를 보냈을시에 나타나는 ATR값의 17번째 바이트의 값이 "00"으로 나타납니다.

ATR: 3B BE 11 00 00 41 01 38 00 00 01 '80' 00 00 00 00 "00" 90 00

위의 submit, select, read, write 명령을 수행하기 위한 **카드 커맨드**는 ACOS3 Reference 메뉴얼의 50페이지에 나와있으며 위의 내용을 간단히 테스트해보고 싶다면 SDK설치시 인스톨되는 Card Tool에서 위의 명령을 보내실 수 있습니다.

3. User Stage 단계 : 본 단계는 일반적인 카드 사용자 모드(엔드유저용)이며 User Stage단계와 User Stage Issuer단계로 구분되어짐. User Stage단계에서 Issuer Code(IC)를 수행하면 Issuer mode(발급자 모드)로 동작모드가 변경되어지며 이때에는 제한적인 메모리 영역에만 접근이 가능함.

◎ **ACOS3카드 EEPROM구조(Internal Data File들의 속성)**

Memory Area	Internal File ID	File Security Attributes			Record Organization
		Manufacturing State	Personalization State	User State	
MCU-ID File	FF 00 _H	R: FREE W: NO ACCESS	R: FREE W: NO ACCESS	R: FREE W: NO ACCESS	2 x 8 bytes
Manufacturer File	FF 01 _H	R: FREE W: IC	R: FREE W: NO ACCESS	R: FREE W: NO ACCESS	2 x 8 bytes
Personalization File	FF 02 _H	R: FREE W: IC	R: FREE W: IC	R: FREE W: NO ACCESS	3 x 4 bytes
Security File	FF 03 _H	R: IC W: IC	R: IC W: IC	R: NO ACCESS W: IC	12 x 8 bytes
User File Management File	FF 04 _H	R: FREE W: IC	R: FREE W: IC	R: FREE W: IC	N_OF_FILE x 7 bytes
Account File	FF 05 _H	R: FREE W: IC	R: FREE W: IC	R: IC W: IC	8 x 4 bytes
Account Security File	FF 06 _H	R: FREE W: IC	R: FREE W: IC	R: NO ACCESS W: IC	4 x 8 bytes
ATR File	FF 07 _H	R: FREE W: IC	R: FREE W: IC	R: FREE W: NO ACCESS	1 X 36 bytes
User File Data Area	File IDs: xx yy _H xx ≠ FF _H	According to the file definitions			

* **MCU-ID File**(FF 00) : 카드 MCU(Micro Control Unit)의 고유번호를 갖고있는 read only 파일, 첫 번째 8byte의 레코드에는 카드 UID가 기록되어있고 두 번째 8byte의 레코드에는 ACOS3카드의 버전 정보 및 카드용량 기록되어있음.

* **Manufacturer File**(FF 01) : Manufacturing단계 이후에는 only read만 가능하며 전자화폐로 사용시에 MAC연산의 영역을 차지하며 또한 카드내 전체 레코드의 수를 표시함.

* **Personalization File**(FF 02) : Personalization 단계에서 User Stage단계로 넘어가고자할 때 이파일의 특정 bit값을 수정하며 또한 User File Area에 새롭게 생성하려는 Record file의 개수를 세팅할때도 사용됨.

* **Security File**(FF 03) : 카드의 보안코드들과 인증키들을 저장하는 파일. ACOS3카드는 총 7개의 보안코드(Issuer Code x 1개, PIN Code x 1개, Application Code x 5개)와 2개의 인증키(카드 인증용 키 x 1개, 단말기 인증용 키 x 1개)가 Security File에 저장됨.

<보안코드의 기능설명>

1. Issuer Code : ACOS3카드의 마스터키로써 이 코드를 알면 원하는 모든 작업이 가능함
2. PIN Code : 엔드유저용 비밀번호로써 일반적으로 은행해서 사용하는 현금카드의 비밀번호와 같은 역할을 함. CHANGE PIN 커맨드로 PIN Code변경 가능.
3. Application Code : ACOS3카드에는 5개의 어플리케이션이 있고 각 Application Data file에 저장되어있는 데이터에 접근을 제어하기 위한 코드임.

※PIN Code와 Application Code는 코드값이 틀렸을 경우 7회까지 재입력이 가능하며 8회 틀렸을시 잠금, 잠금을 풀기위해서는 Security File을 Select하여 Issuer Code를 수행한 후, Security File의 11번과 12번(백업용) record에 저장되어 있는 에러카운터를 0으로 리셋할수 있음. 단, IC(Issuer Code)의 경우에는 8회 틀렸을시 카드에 더 이상 작업할수 없음.

* **User File Management File**(FF 04) : User File Area에 새롭게 생성되는 User File의 파일이름, 한 개 record의 길이, record 개수를 저장함.(ACOS3 Reference 매뉴얼의 20페이지 참조)

* **Account File**(FF 05) : 전자통장, 전자화폐와 같은 어플리케이션에서 금액 및 계좌와 관련된 데이터를 저장하는 파일로써 이 파일의 option bit값을 세팅하지 않을 경우 COS(Card O/S)에서 처리되지않으므로 이 영역을 User File 영역으로 활용 할 수 있음.

* **Account Security File**(FF 06) : MAC암호화 checksum의 연산용으로 사용되어지는 네 개의 보안키가 저장되는 파일로써 이 파일의 option bit값을 세팅하지 않을 경우 COS(Card O/S)에서 처리되지않고 User File 영역으로 활용 할 수 있음.(Personalization단계의 종료후에는 read/write 불가)

* **ATR File**(FF 07) : ATR값과 관련된 정보저장. 카드에 reset신호를 보내면 되돌아오는 응답값인 ATR값을 개발자가 ATR File에 값을 write하여 마음대로 설정할 수 있음, ATR File의 첫 번째 바이트의 세팅으로 ACOS3카드의 통신속도(9,600bps~223,200bps)를 변경가능하며 변경된 값은 reset신호 이후에 적용되어짐.(ATR값 설정관련해서 ACOS3 Referece 매뉴얼의 11페이지 참조)

* **User File**(xx yy) data area : User File Management File에서 설정한 User File이 실제 저장되는 영역.

< IC카드안의 파일 종류와 text데이터의 write/read 샘플코드 >

* 일반적으로 IC카드는 MCU타입(CPU+COS가 포함되어 스스로 연산가능)과 메모리형(CPU와 COS없이 단순히 EEPROM만 있음)의 두가지로 나뉘어지며 메모리내의 파일구조 또한 차이가 있습니다. MCU타입 카드는 파일구조를 Record file(Linear fixed file)형태와 Binary file(Transparent file)형태 모두 사용할 수 있으며 메모리형 카드는 카드내의 EEPROM 전체가 하나의 Binary file이라고 보면 됩니다. Record file과 Binary file을 비교하면 Record파일은 아래 그림2)처럼 줄이 쳐져있는 공책의 개념으로 한개 Record의 길이(한줄의 길이)와



Record의 총 개수(공책 줄의 총 개수)를 지정하실수 있습니다. 장점은 데이터를 read/write 할 때 특정 번지를 기억할 필요없이 파일의 record를 선택해주면 됩니다. 이때 한 record의 최대 길이는 ISO7816 part3 규정에 따라 255byte가 최대입니다. 따라서 대용량의 데이터를 저장하기 위해서는 데이터를 255byte로 잘라서 넣어야합니다.

아래는 ACOS3카드에서 Record file구조를 사용하여 "I AM A BOY"란 text를 write/read하는 APDU 커맨드 샘플입니다. APDU 커맨드는 PC/SC API중에 SCardTransmit() 함수를 사용하여 IC카드에 명령을 보낼수 있습니다.(PC/SC API 관련 샘플은 SDK 설치시 복사되는 WWSample CodesW~~~~각 language~~~WSimple PCSC 폴더의 샘플을 참고하시기 바랍니다.)

 .RESET

;submit Issuer Code(41 43 4F 53 54 45 53 54 = ACOSTEST)

80 20 07 00 08 41 43 4F 53 54 45 53 54

;select Personalization File(FF 02)

80 A4 00 00 02 FF 02

;write record(2개의 file을 만들기 위해 Personalization file의 0번 record에 02 writing함)

80 D2 00 02 01 02

;select User File Management File(FF 04)

80 A4 00 00 02 FF 04

;write record(file 이름 BB 22 / 한개 record 길이 0F / record 총 개수 0F/ 의 User File을 생성하기 위해 User File Management File에 writing함, 00은 Record file구조의 Flag값, 관련정보는 ACOS3 Reference 메뉴얼의 20페이지 참고)

80 D2 00 00 07 0F 0F 00 00 BB 22 00

;select BB 22 file

80 A4 00 00 02 BB 22

:write record(BB 22 file의 02 record(세번째 record) "I AM A BOY" writing함)

80 D2 02 00 07 49 41 4D 41 42 4F 59

:read record(BB 22 file의 02 record(세번째 record)에서 7byte 길이의 데이터 읽음)

80 B2 02 00 07

반면, Binary file의 경우 위의 그림1)과 같이 줄이 쳐져있지 않은 한 장의 무제공책으로 이해할수 있습니다. SLE5528(1Kbyte), SLE5542(256byte)같은 메모리형 카드가 한개의 Binary file로 되어있는 구조입니다. 장점은 얼마의 데이터를 저장할지 정해지지 않을 경우 단지 메모리 번지만 선택하여 원하는 길이만큼 write/read하면 됩니다.

아래는 ACOS3카드에서 Binary file구조를 사용하여 "I AM A BOY"란 text를 write/read하는 샘플코드입니다.

.RESET

:submit Issuer Code(41 43 4F 53 54 45 53 54 = ACOSTEST)

80 20 07 00 08 41 43 4F 53 54 45 53 54

:select Personalization File(FF 02)

80 A4 00 00 02 FF 02

:write record(2개의 file을 만들기 위해 Personalization file의 0번 record에 02 writing함)

80 D2 00 02 01 02

:select User File Management File(FF 04)

80 A4 00 00 02 FF 04

:write binary(file 이름 BB 22 / binary file사이즈 256byte(01 00)의 User File을 생성하기 위해 User File Management File에 writing함, 80은 Binary file구조의 Flag값, 관련정보는 ACOS3 Reference 메뉴얼의 20페이지 참고)

80 D2 00 00 07 01 00 00 00 BB 22 80

:select BB 22 file

80 A4 00 00 02 BB 22

:write binary(BB 22 file의 00 00번지에 "I AM A BOY" writing함)

80 D0 00 00 07 49 41 4D 41 42 4F 59

:read binary(BB 22 file의 00 00번지에서 7byte 길이의 데이터 읽음)

80 B0 00 00 07

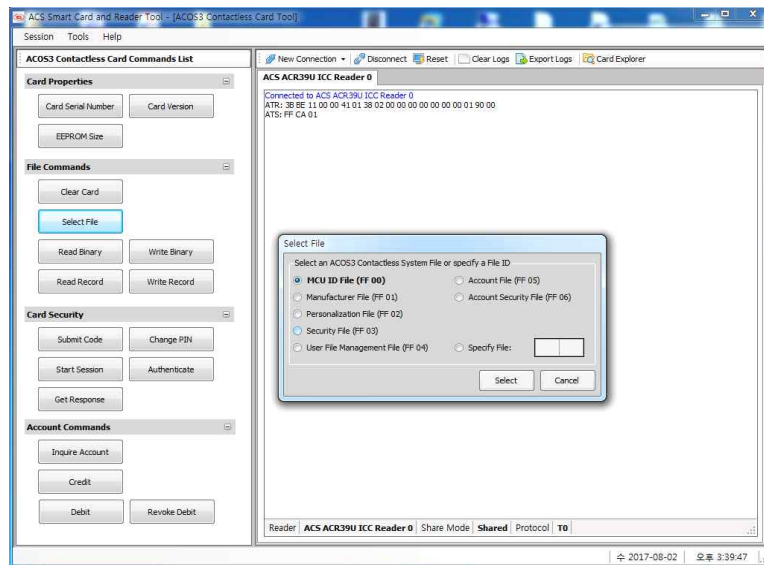
◎ ACOS3용 카드command

Command	INS	설 명
Start Session	84	세션키를 생성하기위해 상호인증 절차를 시작함.
Authenticate	82	ACOS3카드에 암호화된 random number를 submit하고 세션키의 연산을 수행함.(카드와 터미널(SAM카드)사이의 상호인증을 수행)
Get Response	C0	ACOS3카드로부터 응답가능한 response 데이터를 얻음.
Submit Code	20	ACOS3카드에 보안코드(Issuer Code, PIN Code, Application Code)를 수행함.
Change PIN	24	PIN코드를 변경함.
Get Card Info	14	ACOS3카드로부터 카드정보(시리얼번호, EEPROM사이즈, 버전정보 등)을 얻음.
Clear Card	30	카드를 초기화함.(카드내의 데이터, 보안코드들, 인증키를 초기화함, 단 Issure Code와 Manufacturer File은 초기화 불가)
Select File	A4	데이터를 read/write하기 위해 특정파일(Internal File 또는 User File)을 select함.
Read Record	B2	현재 select된 file에서 특정 record파일의 데이터를 원하는 길이만큼 read함.
Write Record	D2	현재 select된 file에서 특정 record파일의 데이터를 원하는 길이만큼 write함.
Read Binary	B0	현재 select된 file에서 특정 binary파일의 데이터를 원하는 길이만큼 read함.
Write Binary	D0	현재 select된 file에서 특정 binary파일의 데이터를 원하는 길이만큼 write함.
Inquiry Account	E4	계좌의 정보(계좌번호, 잔액 등)를 읽어옴.
Credit	E2	계좌로 금액을 입금함.
Debit	E6	계좌에서 금액을 출금함.
Revoke Debit	E8	가장 마지막으로 수행된 출금을 취소함.

◎ ACS Smart Card and Reader Tool

- **ACS Smart Card and Reader Tool** : ACR39U리더기 및 접촉식카드로 제품 개발시 직접적인 APDU커맨드를 보내지않고 이미 만들어진 툴 상의 아이콘을 클릭하여 직접적으로 카드에 명령을 내릴수 있는 매우 유용한 도구입니다. 위에서 알아본 **sample code**의 명령들은 CardTool상에서 실행가능하며 좀더 편하게 Record file의 **select**, 보안코드의 **submit**, Record 내용의 **read / write** 할 수 있고 그에 대한 응답값이 나타나며 동시에 PIN코드 변경도 가능합니다. 에러발생시에는 log창에 나타나는 리턴값을 통한 분석이 가능합니다.

지원되는 리더기 : ACR39U, ACR39T, ACR38, ACR38K, ACR38T, ACR38DT, ACR38ET, ADT60, AET60, AET63 and ACR80.



◎ Sample Codes

ACR39U-SDK는 아래와 같이 다양한 language별 샘플 코드를 제공하여 개발자분들에게 좀더 편한 개발 환경을 제공합니다.

* 제공되는 샘플의 language : ActiveX, Java, Linux C++, MS VB .NET 2013, MS Visual C# 2013, MS Visual C++ 2013(64bit), MS Visual C++ 6.0(32bit),

- Cards Programming 폴더

ACOS3 폴더 : ACOS3 카드내의 Internal 데이터영역에 어떻게 User File을 생성하는지, 생성된 User File에 어떻게 값을 읽고 쓰는지와 암호화(DES 또는 3DES)옵션 적용, ACOS3카드와 단말기(SAM슬롯의 SAM카드)간의 상호인증을 위한 샘플코드 외에 ATR값을 얻고 ATR을 특정값으로 세팅시킬수있는 샘플코드가 ACOS3폴더 내에 들어있습니다.

※ ATR (Answer To Reset) : 리셋 신호에 대한 응답 데이터값 (스마트 카드가 리더기에 삽입되면 외부 장치로부터 보내오는 명령어에 따라서 리셋 작업을 수행하며, 리셋 작업의 결과로 카드의 종류, 모델, 제조사 등의 정보를 담고 있는 리셋 응답 데이터값(ATR)를 받게됨. ATR이 정상적으로 리턴되면 카드와 리더기사이에서 정상적인 통신이 가능한 상태임을 나타냄.

SLE Memory Cards 폴더 : 메모리형 카드(SLE5528, SLE5542)의 EEPROM에 데이터 읽기, 쓰기, 쓰기방지, PIN Code값 변경등을 구현할수 있는 샘플코드가 포함되어 있습니다.

- 기타 폴더 : ATR값을 얻는 간단한 샘플, 리더기내에 카드가 삽입되어졌는지의 삽입여부를 detect하는 폴링(Polling)샘플, PC/SC 국제표준 API중에 가장 많이 사용되고 필히 사용되어야하는 API만을 모아놓은 Simple PCSC샘플코드가 포함되어 있습니다.

◎ **SLE5542 Momory Cards** (관련정보는 Manual의 8.4 참고. 29~33)

- **Memory** 구조 : 메모리형 카드는 read는 free지만 write는 Secret code를 제공(submit)한 후에 write작업이 가능합니다.

<p>The diagram illustrates the memory structure of the SLE5542 chip. It is divided into three main sections: MAIN MEMORY, PROTECTION MEMORY, and SECURITY MEMORY. MAIN MEMORY is further divided into an application area (addresses 32-255) and a manufacturer area (addresses 0-31). PROTECTION MEMORY is a 32-bit area. SECURITY MEMORY contains a 3-byte card secret code and a counter. The diagram shows the interconnections between these areas.</p>	<ul style="list-style-type: none"> ▶ 256byte EEPROM ▶ 3byte Secret Code (3bits Error Counter) ▶ 32bit Memory Protection ▶ 자유롭게 읽기 가능
<p>MAIN MEMORY</p>	<p>manufacturer area</p> <ul style="list-style-type: none"> ·chip 제조업체 정보 ·chip 종류와 버전 ·card 제조업체 정보 ·card serial number ·이 영역은 /삭제가 잠겨 있음 <hr/> <p>application area</p> <ul style="list-style-type: none"> ·Secret code(PSC:Programmable Security Code) 인증후 쓰기/삭제가 가능
<p>PROTECTION MEMORY</p>	<ul style="list-style-type: none"> ·32byte의 제조사 영역(manufacturer area)을 보호하기위해 1bit를 사용 ·Protection bit : 데이터의 해당 주소를 전송하여 보호설정
<p>SECURITY MEMORY</p>	<ul style="list-style-type: none"> ·4byte EEPROM (3byte Secret Code, 3bit Error Counter) ·Secret Code 인증 후 읽기 가능. ·잘못된 Secret Code는 Error Counter를 발생시킵니다.(3회 오류시 잠김)

- **Error Counter 확인** (관련정보는 Manual의 8.4.3 참고)

07 FF FF FF 90 00	정상 (3회 남음)
03 00 00 00 90 00	1회 틀림 (2회 남음)
01 00 00 00 90 00	2회 틀림 (1회 남음)
00 00 00 00 90 00	3회 틀림 (사용 못함)

* Secret code를 3번 이상 잘못 넣으면 카드가 잠겨서 사용이 불가능 합니다. 그러나 1~2번 틀리더라도 정확한 값을 넣으면 다시 에러카운트가 초기화 됩니다.

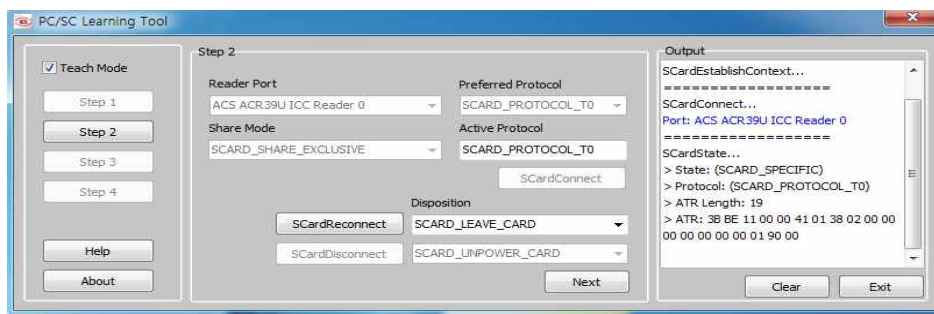
- **Secret code 변경** (관련정보는 Manual의 8.4.8 참고)

CLA	INS	P1	P2	ME M_L	CODE		
					byte 1	byte 2	byte 3
FF	D2	00	00	03			

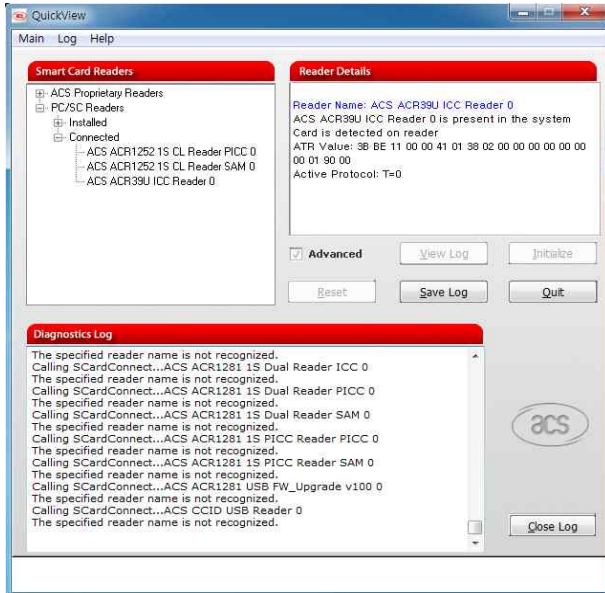
* 이 명령어는 PRESENT_CODE(Secret Code)가 입력된 상태에서만 가능합니다.

◎ Tools and Utilities

- **PC/SC Learning Tool** : PC/SC표준 API를 단계에 따라서 어떻게 사용하는지와 어떤 API부터 수행해야하는지, 또한 어떤 파라미터들을 사용해야하는지 보여주는 도구입니다.



- **QuickView** : ACS의 접촉식 리더기의 드라이버가 정상적으로 install 되어졌는지, 삽입된 카드가 정상적으로 동작하는 카드인지(RESET신호를 보내서 ATR값이 잘 return되는지 확인) 체크해주는 유틸리티입니다.



- **Scripting Tool 3** : 사용하고자하는 APDU커맨드를 텍스트창에 직접 입력하여 결과값을 확인할 수 있는 툴입니다. 참고용으로 만들어져 있는 샘플 스크립트를 불러와서 실행시켜볼 수도 있습니다.

(C:\...~\ACR39U SDK\Tools and Utilities\Script Tool 4 밑에 샘플스크립트가 있으니 참고하시기 바랍니다.)



◎ **User Manuals and Reference Materials** (관련 메뉴얼 및 참고자료)

※ 자료는 모두 *.PDF 형태이며 Acrobat Reader는 CD의 Step5.단계에서 설치하실 수 있습니다.

- **ACOS3 Reference Manual** : ACOS3카드의 특징, 기능, 내부구조, Internal file들의 구성 및 속성, 카드 command 및 응답값에 관한 세부 매뉴얼로써 개발관련된 모든 내용이 들어있는 핵심 매뉴얼.
- **ACR39x Reference Manual** : ACR39U 리더기의 리더 command 정리 및 메모리형 카드에 작업시 각 카드별 메모리구성과 select, read/write 관련된 커맨드의 매뉴얼.
- **ACR39U SDK User Manual** : 현재 읽고있는 메뉴얼의 영문판으로 ACR39U-SDK의 구성과 관련된 매뉴얼.
- **ACR39U-U1 Technical Specifications** : ACR39U리더기의 기능, 특징 및 표준스펙이 사진과 함께 간단히 설명되어 있음.

◎ **스마트카드 관련 약어**

스마트카드 약어	
ACK	Acknowledge 승인 응답문자 : 데이터 전송이 성공이면 ACK코드값을 되돌려 받음.
APDU	Application Protocol Data Unit 스마트카드에서 사용하는 응용 프로토콜 데이터 단위(스마트카드와 리더기간의 데이터 교환 형식)
ATQA	Answer To Request, type A 요청에 의한 응답, ISO14443 Type A 카드로부터의 요청에 의한 응답
ATQB	Answer To Request, type B 요청에 의한 응답, ISO14443 Type B 카드로부터의 요청에 의한 응답
ATR	Answer To Reset 스마트카드에 보내진 리셋신호 대한 응답값으로 ISO 7816 표준으로 정의되어짐. 스마트 카드가 리더기에 삽입되면 외부 장치(PC등)로부터 보내오는 명령어에 따라서 리셋 작업을 수행하며, 리셋 작업의 결과로 카드의 종류, 모델(버전), 제작 회사 등의 정보를 담고 있는 응답신호(ATR)를 외부장치로 보냄. 외부장치<->리더기<->스마트카드간의 최초 정상통신 및 동작여부를 확인할 수 있는 응답값
ATS	Answer To Select Select 명령을 보냈을 때 리턴되는 응답값
CCID	Chip/Smart Card Interface Device 스마트카드 장치(리더기)에 관련된 표준규격으로 Microsoft에서는 Windows Vista이상버전의 O/S는 기본적으로 CCID드라이버를 탑재하고 있어서 제조사쪽에서 제공하는 별도의 장치(리더기)드라이버를 설치할 필요가 없음.
COS	Card Operating System(스마트카드 운영체제) 스마트카드 운영체제(O/S)는 크게 두가지로 나뉘는데 개방형 플랫폼과 폐쇄형 플랫폼이 있음. 개방형카드의 종류는 크게 MULTOS(Multi-Application Operating System)와 Java카드(Global platform)가 있으며 폐쇄형 카드는 Proprietary(전용) O/S를 사용하는 카드를 일컫음. MULTOS: 1996년 Mondex사가 개발하고 MASCO산업 컨소시엄이 지원하는 다기능 COS로 MULTOS의 COS위에 MULTOS의 인터프리트 언어인 MEL로 설계된 MEL가상머신을 탑재한 형태의 스마트카드 플랫폼 Java 카드: 자바카드는 COS위에 SUN사가 개발한 자바가상머신(JVM)을 탑재한 형태의 스마트카드 플랫폼으로 현재 Javacard 버전 2.2.1 사용되고 있음.

EMV	Europay / Master card / Visa card 세계 3대 신용 카드 회사인 벨기에의 유로페이, 미국의 마스터 카드, 비자 카드 등 3개사가 공동으로 결제하는 IC 카드의 표준 규격. 이름은 3개사의 머리글자를 따서 붙여짐. 미국의 아메리칸 익스프레스 등 다른 카드 회사도 이 규격을 지지하고 있으며, IC 카드형 전자 화폐를 대표하는 사실상의 표준 EMV인증은 H/W(스마트카드단말기)와 관련된 EMV2000 Level1 인증과 S/W(단말기펌웨어, 결제모듈)와 관련된 EMV2000 Level2 인증이 있음
NAK	Negative Acknowledge 부정 응답문자 : 데이터 수신에 에러가 있음을 확인하는 신호.
PC/SC	Personal Computer/Smart Card 종류가 다른 스마트카드와 PC간의 상호 호환을 위해 Microsoft, HP, Sun Microsystems등 의 7개사 Workgroup을 결성하여 PC/SC란 표준규격을 제정함. 이 표준규격은 제조회사가 다른 스마트카드와 리더기사이에 상호 호환을 준수하며 다중응용프로그램간에 자원공유를 가능하게함으로써 H/W구매 비용과 개발비용을 줄여주고 있음. 현재 PC/SC 1.0버전이 사용되고 있음(PC/SC part 1~8) PC/SC 구조는 Interface Device Handler, ICC Resource Manager, Service provider로 구성됨 - Interface Device Handler : 리더기를 위한 장치드라이버로써 리더기의 기능을 I/O인터페이스로 매핑시키는 역할을 수행함. - ICC Resource Manager : PC에서 사용하는 스마트카드와 리더기로의 모든 접근을 조정 및 제어하고 스마트카드와 관련된 모든 자원을 관리함. (Windows시리즈의 경우 ScardSvr.exe, ScardSvr.dll) - Service Provider : 특정 스마트카드에서 제공되는 기능을 캡슐화하고 API를 통하여 어플리케이션이 스마트카드로 접근할수 있도록 함.(Windows용 스마트카드 API는 winscard.dll에 구현 되어있음)
PCSC Lite	Personal Computer/Smart Card Lite Linux용에서 규정된 스마트카드 표준으로 Windows용 PC/SC 구조 및 PC/SC API와 유사
PICC	Proximity Integrated Circuit Card Contactless Card로써 RFID카드를 지칭함. ICC는 접촉식 카드
PIN	Personal Identification Number 스마트카드에 저장되어지는 개인별 식별(보안) 번호로 8자리 숫자로 구성됨.
R-APDU	Response APDU 응답 APDU
REQA	REQuest Answer, type A ISO14443 Type A카드에 대한 응답 요청
REQB	REQuest Answer, type B ISO14443 Type B카드에 대한 응답 요청
SAK	Select Acknowledge, type A Type A의 카드타입 응답값
SAM	Secure Access Module 카드 판독기(리더기) 내부에 장착되어 카드와 단말기의 유효성을 인증하고 통신 데이터를 암호화하여 정보의 노출 방지 및 통신 메시지의 인증 및 검증함. 또한 카드에서 이전된 전자적인 가치를 저장하기도 함. 인터넷 전자 상거래 시 또는 개인용 컴퓨터(PC) 사용 시 프로그램 안에 카드 인증용 SAM을 내장하기도 한다
SIM	Subscriber Identity Module(가입자 인증 모듈) 휴대폰에서 사용되는 가입자(사용자) 정보를 저장하는 커팅된 스마트카드의 일종
T=CL	ISO/IEC14443 part4를 지원하는 RFID카드에서 사용하는 프로토콜 접촉식카드의 ISO7816 part4 에서 사용하는 전송 프로토콜과 유사
WUPA	ISO14443 TypeA용 Wake-Up Command
WUPB	ISO14443 TypeB용 Wake-Up Command