Smart Card APDU Analysis

Black Hat Briefings 2008
Las Vegas

Ivan "e1" Buetler

ivan.buetler@csnc.ch

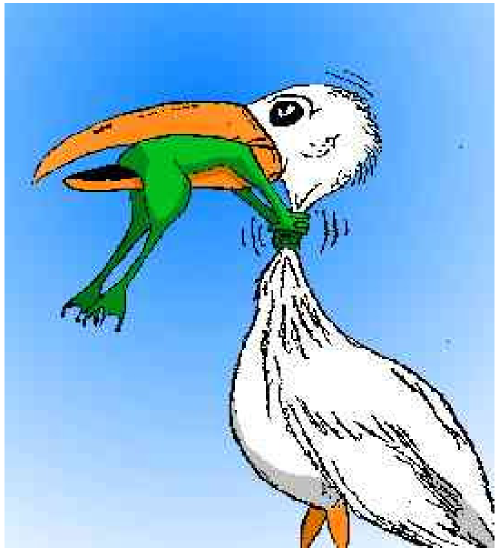
Compass Security AG - Switzerland

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

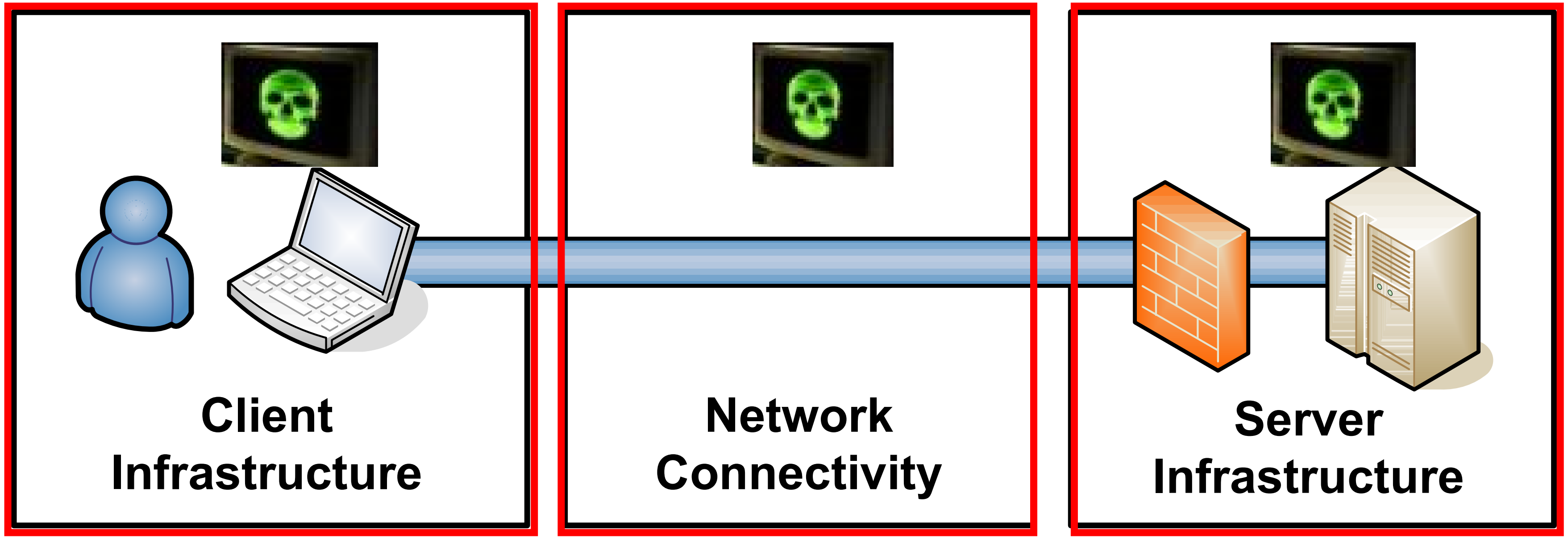
Hypothesis::Statement

SOFTWARE
cannot protect
SOFTWARE



Hypothesis::Situation

Attacker Toolkit: *Please choose your victim…*



Victim 1:
E-Mail Contamination
Visits to malicious Web Sites
Second Channel Attacks

Victim 2:
Phishing, Pharming
DNS Spoofing
Network Interception

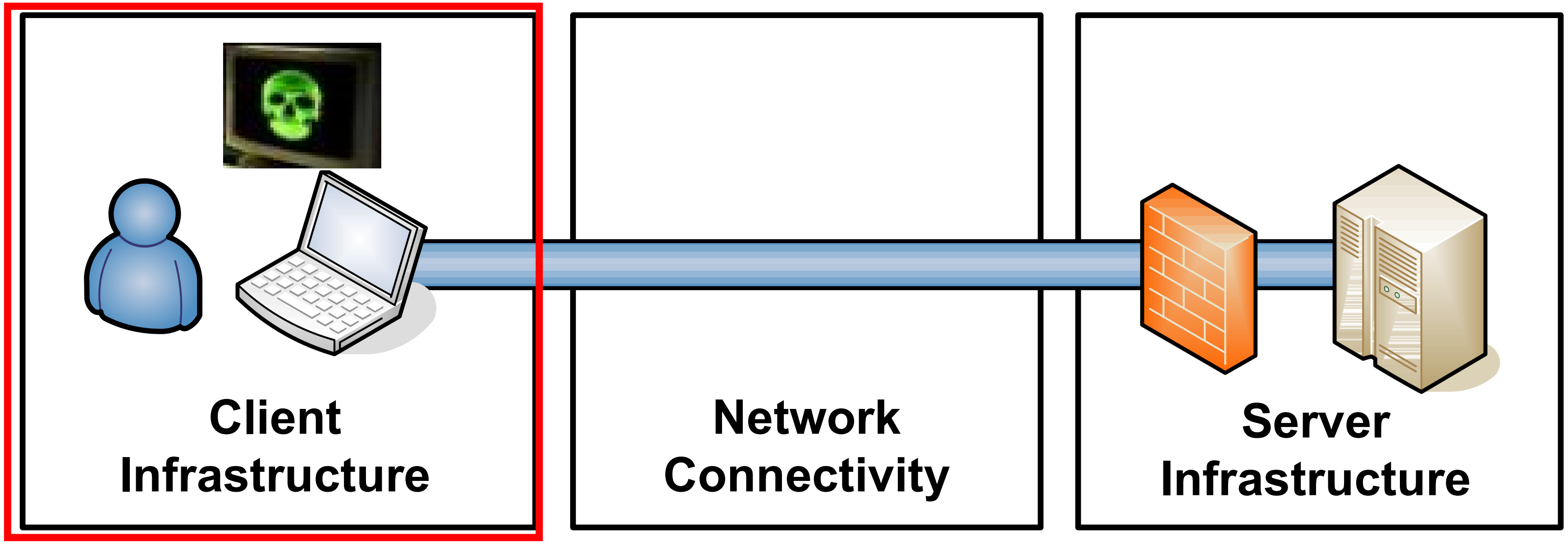
Victim 3:
Web 2.0 Hacking
Cross Site Scripting …
Malicious Web Sites

Hypothesis::Situation

E-Mail

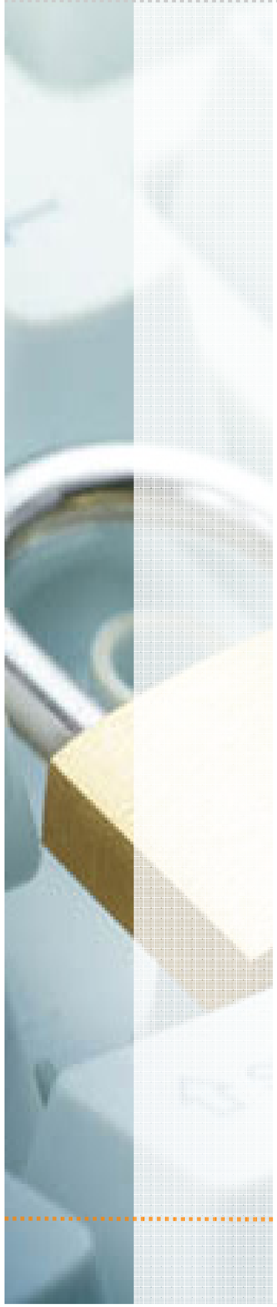
Malicious
Web Site

Attacker Toolkit: *Please enter the attacking strategy …*



Most promising target

-> Client Computer



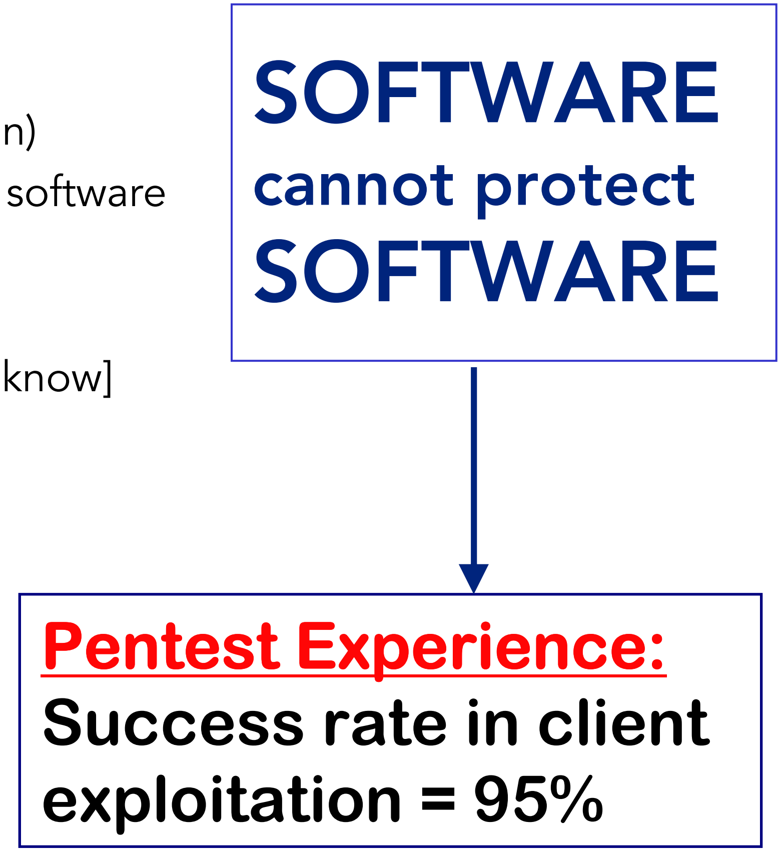
Hypothesis::Situation

Client Infection Approaches

- E-Mails
- Malicious Web Sites
- Rogue Access Points (drive-by-injection)
- Exploitation of internet enabled client software
- Malicious U3, USB stick
- Malicious CD-Rom
- .... [many infection strategies – as you know]

Client Security Defense Strategies

- Latest patches / Update services
- Firewall / Personal Firewall
- Anti-Virus protection
- Spyware protection
- Device Locking Suite
- Hard disk encryption



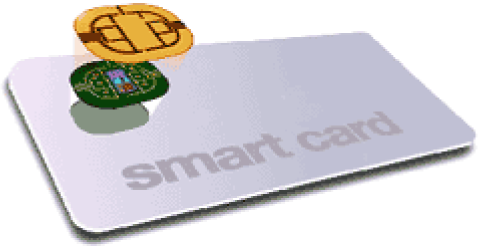
SOFTWARE cannot protect SOFTWARE

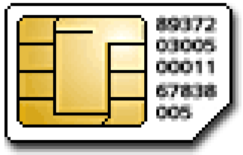
Pentest Experience:

Success rate in client exploitation = 95%

Hypothesis::Conclusion

We need *Secure Devices* - *Tamper Proof* – *Trusted Minicomputers*





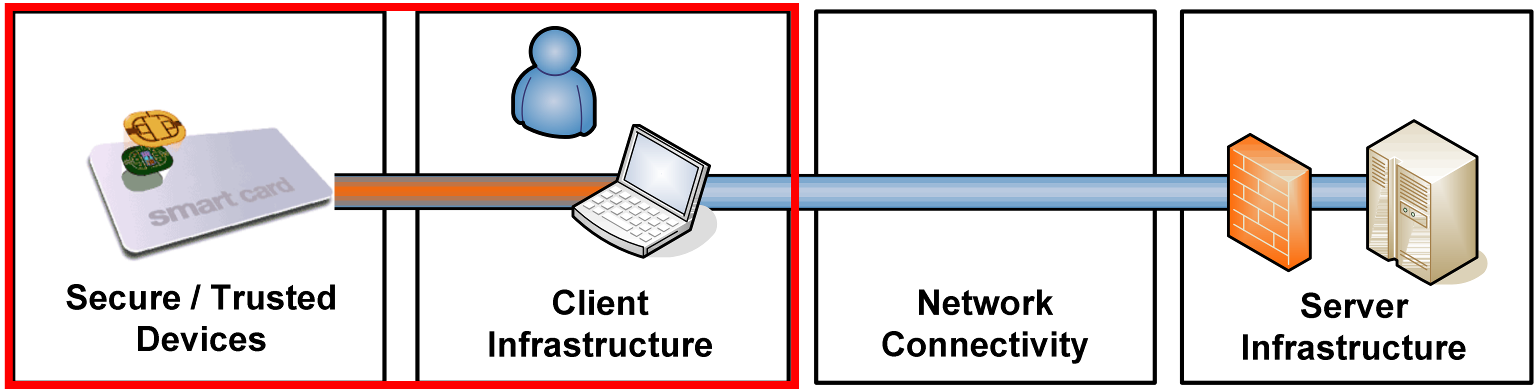
Hypothesis::Conclusion

Secure devices provide ...

- Authentication
- Encryption
- Signatures

Secure devices are ...

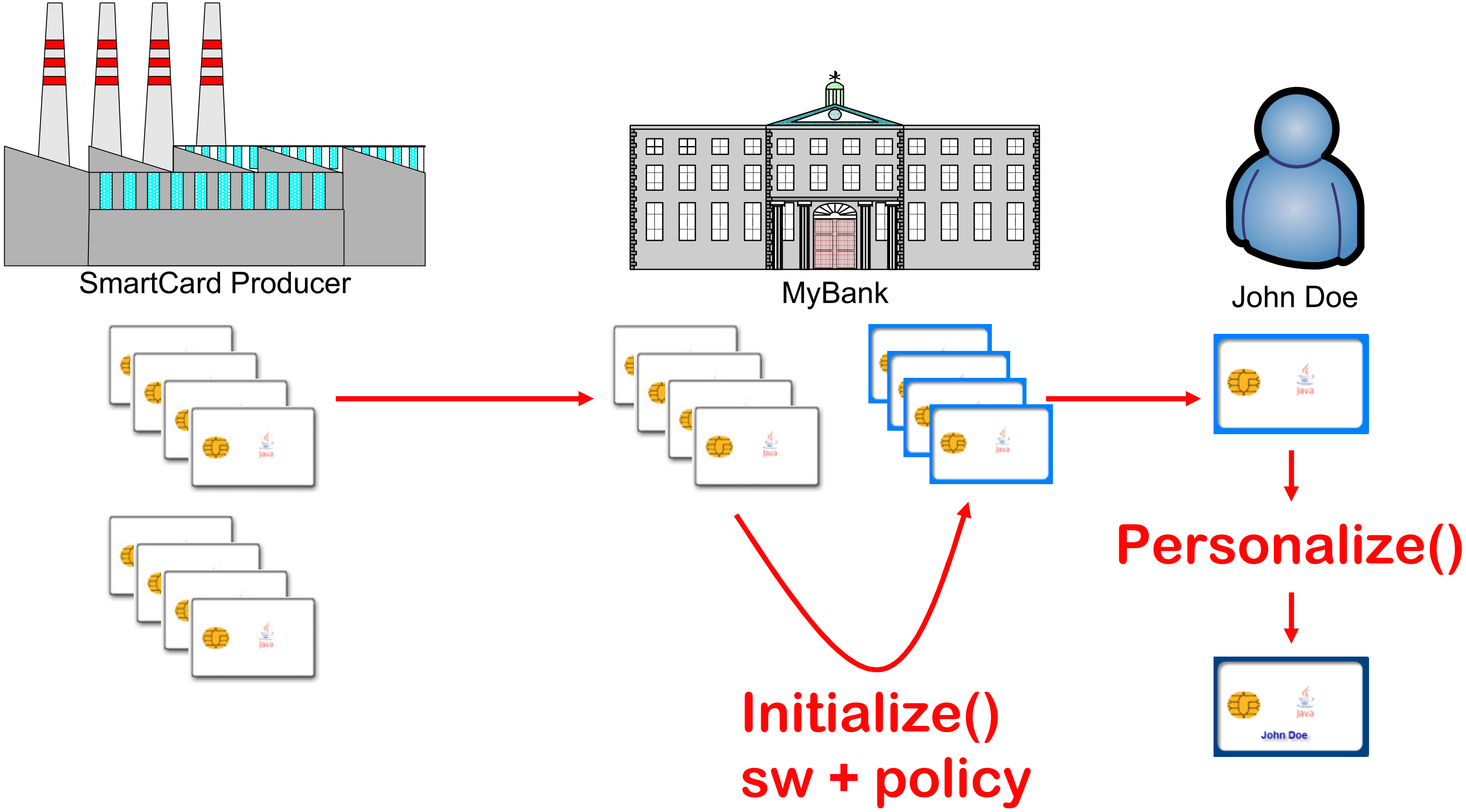
- Tamper Proof
- Virus/Trojan resistant



Smart Card Life Cycle

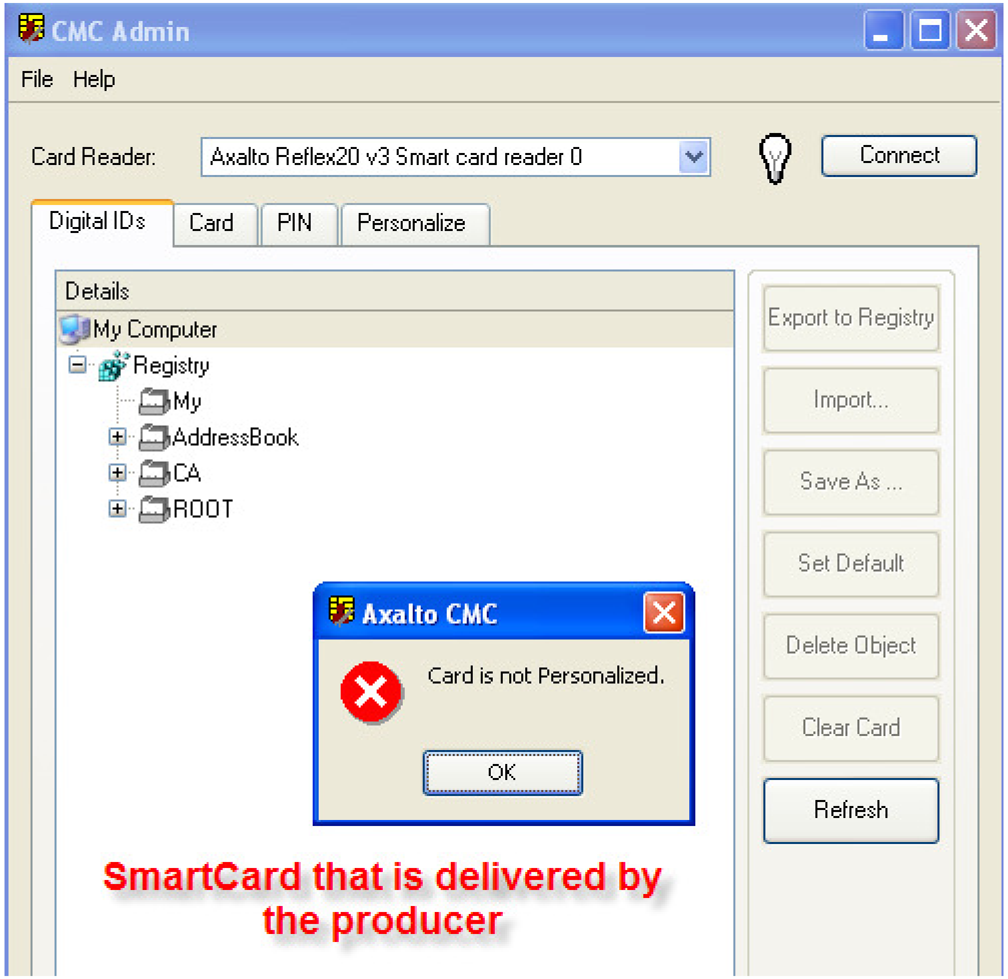
Smart Card::Life Cycle

Producer -> Company -> User



Smart Card::Life Cycle::Initialize()

MyBank::Unitialized Smart Card



Card is not Personalized.

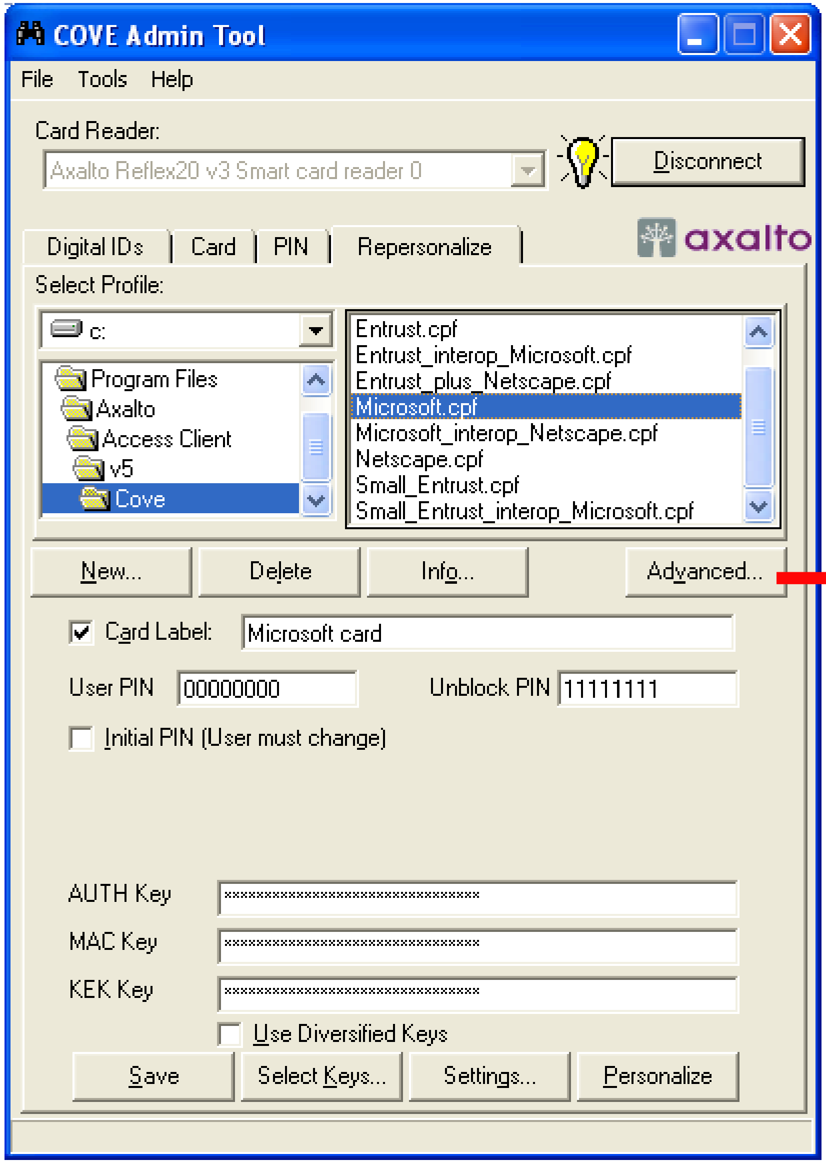
SmartCard that is delivered by the producer

Smart Card needs to be initialized before usage!

Initialization means:

a) PIN policy
b) PUK policy
c) Key generation
d) MasterKeySet
… and more…see next page

Smart Card::Life Cycle::Initialize()



Card Reader: Axalto Reflex20 v3 Smart card reader 0

Select Profile: c:

- Program Files
  - Axalto
    - Access Client
      - v5
        - Cove

Entrust.cpf
Entrust_interop_Microsoft.cpf
Entrust_plus_Netscape.cpf
Microsoft.cpf
Microsoft_interop_Netscape.cpf
Netscape.cpf
Small_Entrust.cpf
Small_Entrust_interop_Microsoft.cpf

☑ Card Label: Microsoft card

User PIN 00000000 Unblock PIN 11111111

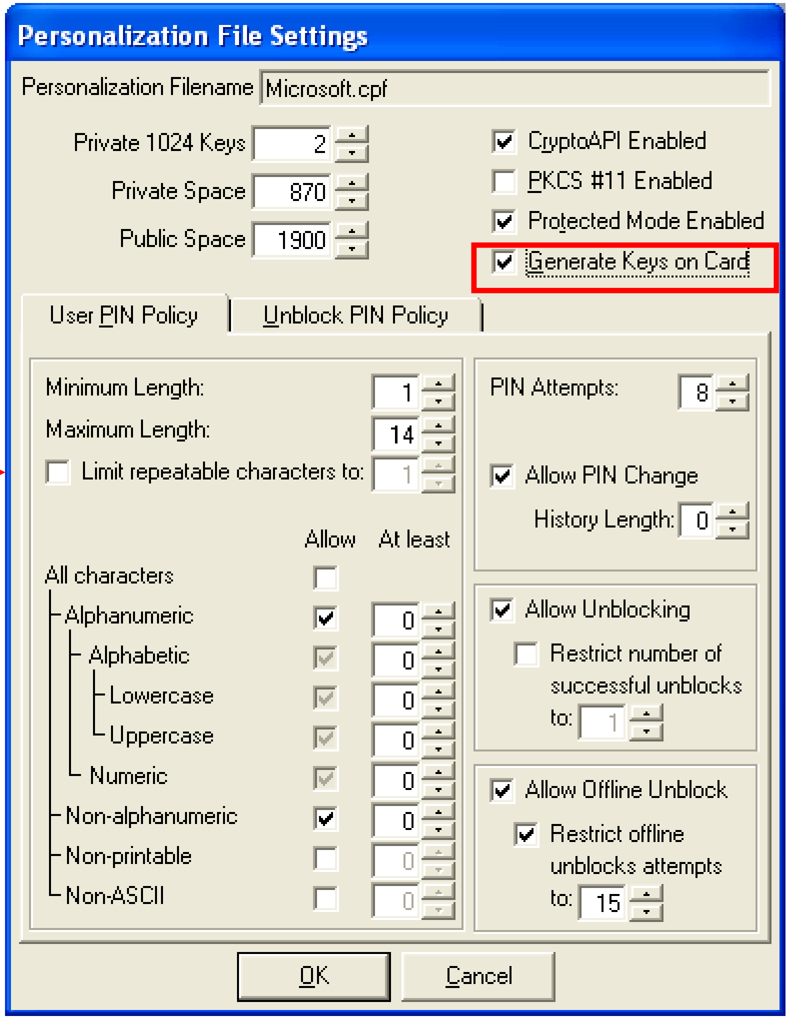
☐ Initial PIN (User must change)

AUTH Key ********************************

MAC Key ********************************

KEK Key ********************************

☐ Use Diversified Keys



Personalization Filename Microsoft.cpf

Private 1024 Keys 2

Private Space 870

Public Space 1900

☑ CryptoAPI Enabled
☐ PKCS #11 Enabled
☑ Protected Mode Enabled
☑ Generate Keys on Card

Minimum Length: 1

Maximum Length: 14

☐ Limit repeatable characters to: 1

	Allow	At least
All characters	☐	
Alphanumeric	☑	0
Alphabetic	☑	0
Lowercase	☑	0
Uppercase	☑	0
Numeric	☑	0
Non-alphanumeric	☑	0
Non-printable	☐	0
Non-ASCII	☐	0

PIN Attempts: 8

☑ Allow PIN Change

History Length: 0

☑ Allow Unblocking

☐ Restrict number of successful unblocks to: 1

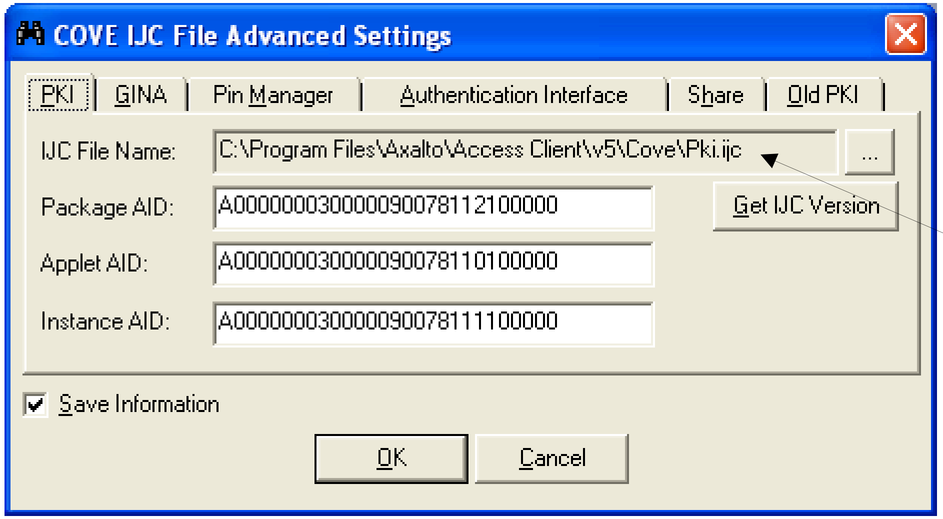
☑ Allow Offline Unblock

☑ Restrict offline unblocks attempts to: 15

Smart Card::Life Cycle::Initialize()

During Initialization...

- Applets are configured (policy)
- Applets are loaded from computer to Smart Card
- Applets are instantiated on Smart Card



COVE IJC File Advanced Settings

IJC File Name: C:\Program Files\Axalto\Access Client\v5\Cove\Pki.ijc

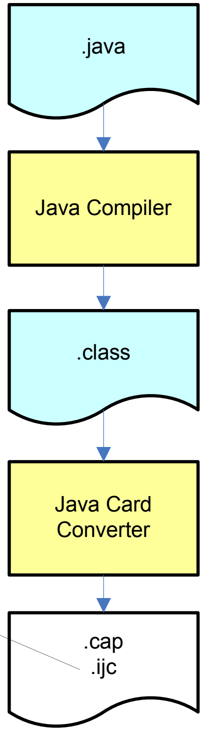
Package AID: A0000000300000900781121000000

Applet AID: A0000000300000900781101000000

Instance AID: A0000000300000900781111000000

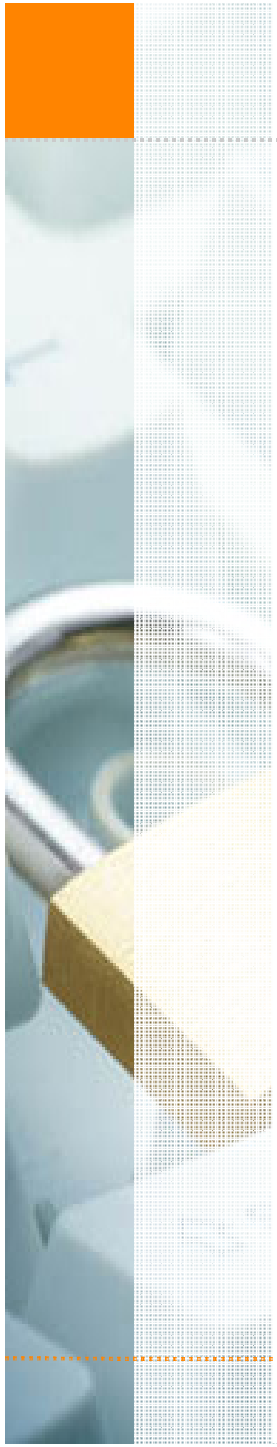
☑ Save Information

Cardlet Development



This is like „initial software package“ on a Personal Computer

- The password for doing so must be known => Master Key Set!!!



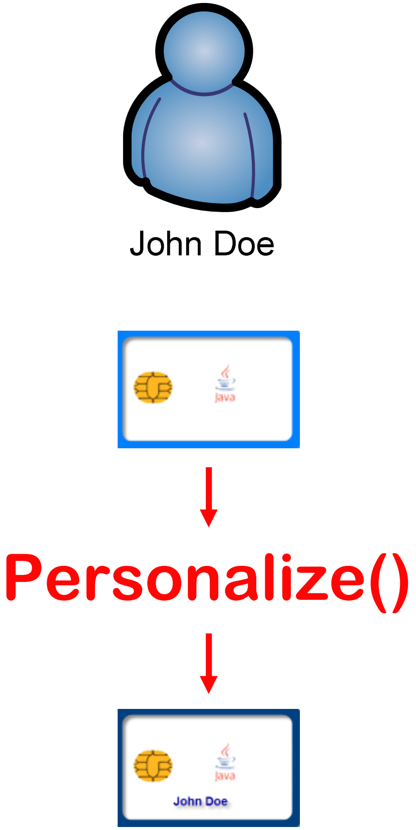
Smart Card::Life Cycle::Personalize()

Certificate Enrollment

- Generate Key on Card
- Generate CSR (certificate signing request)
- Send CSR to CA (certification authority)
- Receive Certificate from CA
- Store Certificate on Card

Smart Card is then useable

- Authentication
- Encryption
- Signatures



John Doe

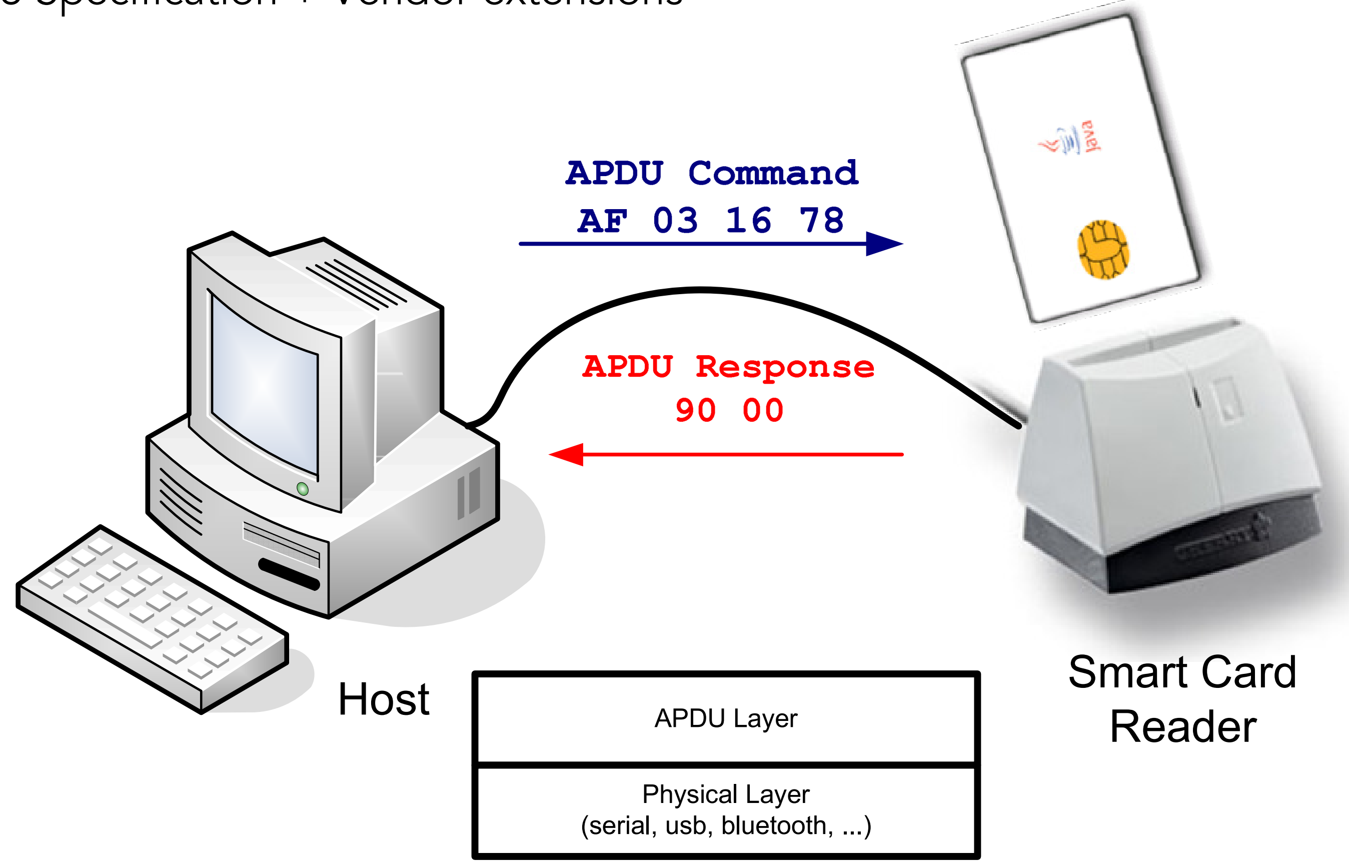
Personalize()

Smart Card
Communication
APDU

Smart Card::APDU

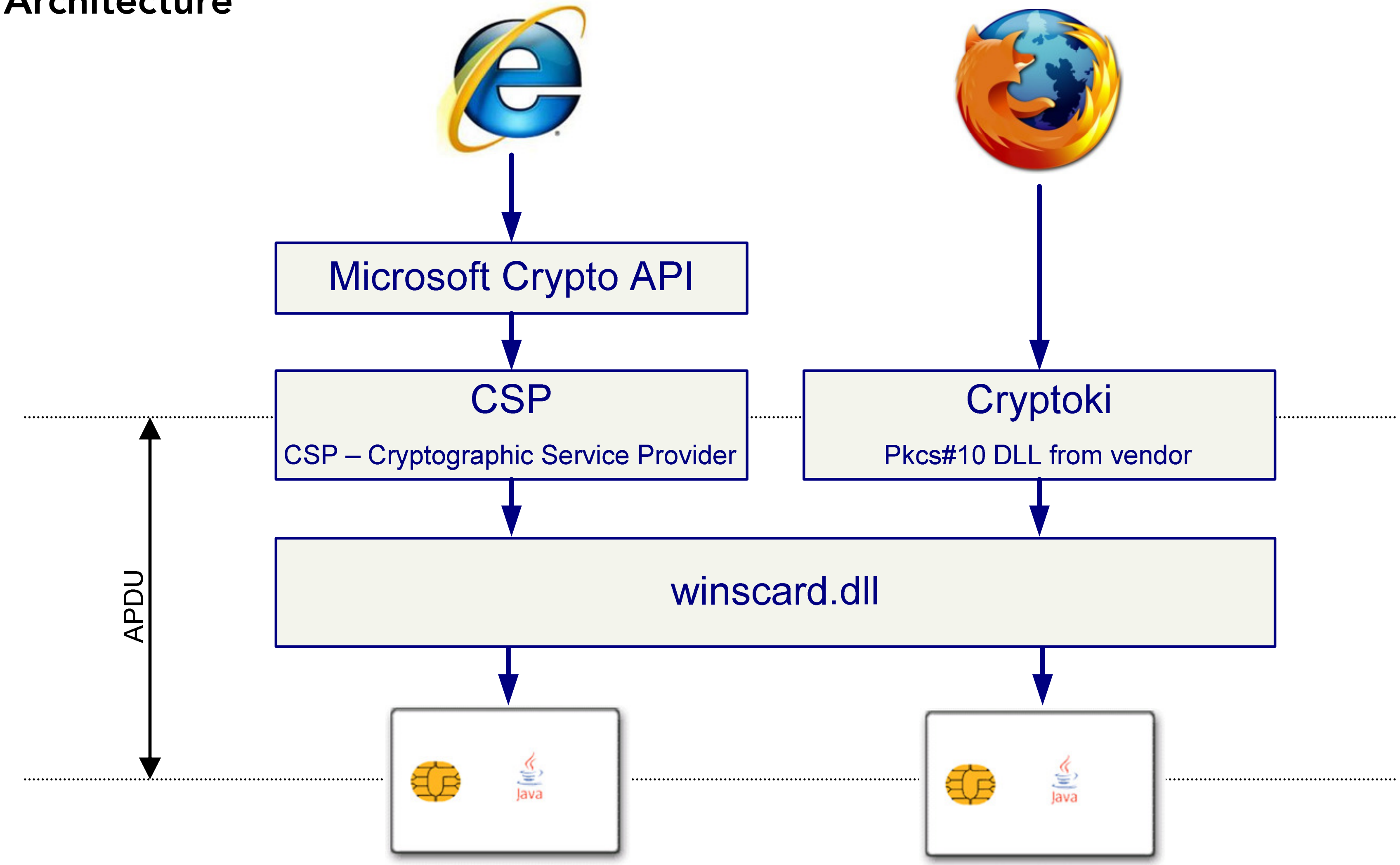
Application Protocol Data Unit

- Communication between CSP/PKCS#10 and Smart Card
- ISO 7816 Specification + Vendor extensions



Smart Card::APDU::Architecture

Architecture



Microsoft Crypto API

CSP

CSP – Cryptographic Service Provider

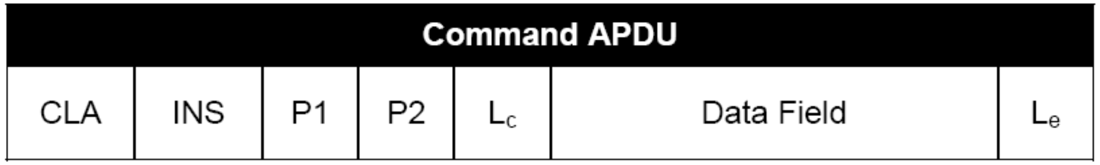
Cryptoki

Pkcs#10 DLL from vendor

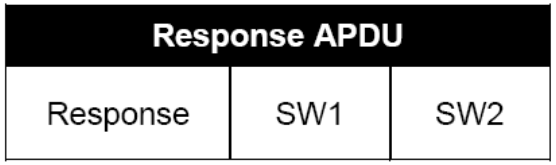
winscard.dll

Smart Card::APDU::Command

APDU Command and Response Structure

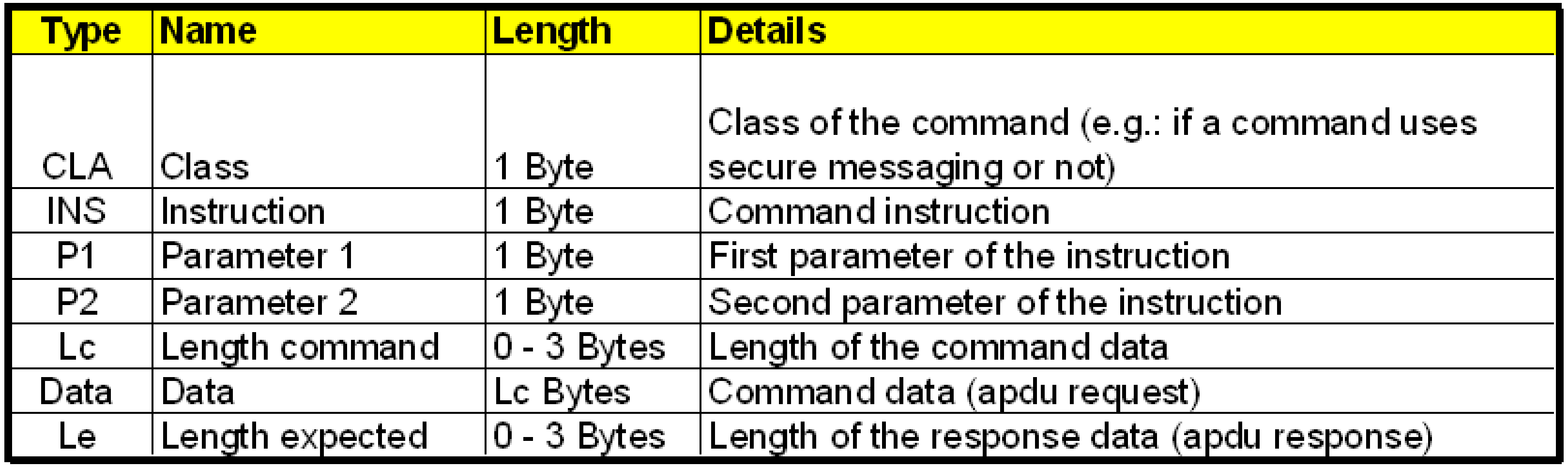


Command APDU						
CLA	INS	P1	P2	L_c	Data Field	L_e

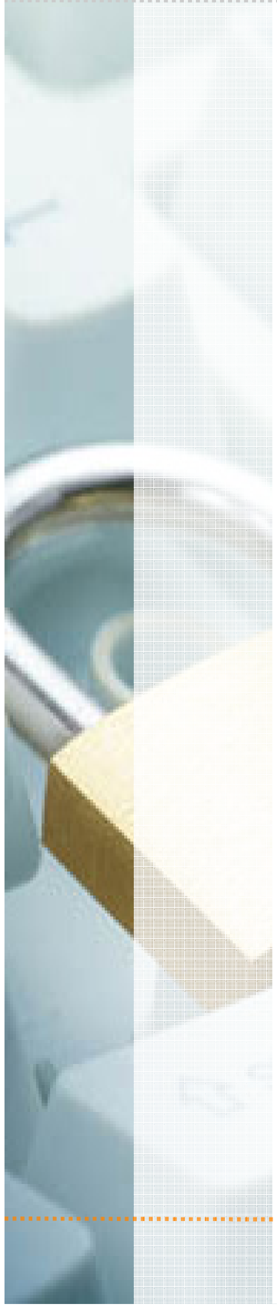


Response APDU		
Response	SW1	SW2

APDU Command Details

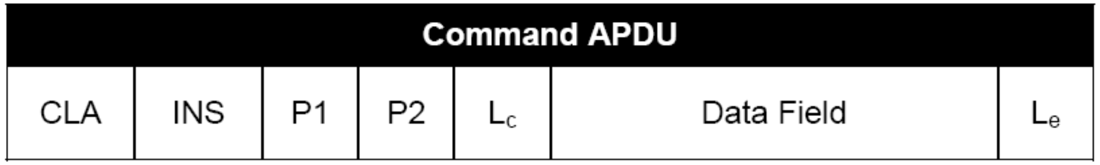


Type	Name	Length	Details
CLA	Class	1 Byte	Class of the command (e.g.: if a command uses secure messaging or not)
INS	Instruction	1 Byte	Command instruction
P1	Parameter 1	1 Byte	First parameter of the instruction
P2	Parameter 2	1 Byte	Second parameter of the instruction
Lc	Length command	0 - 3 Bytes	Length of the command data
Data	Data	Lc Bytes	Command data (apdu request)
Le	Length expected	0 - 3 Bytes	Length of the response data (apdu response)

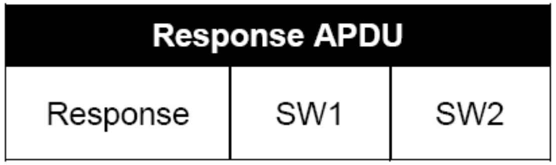


Smart Card::APDU::Response

APDU Command and Response Structure

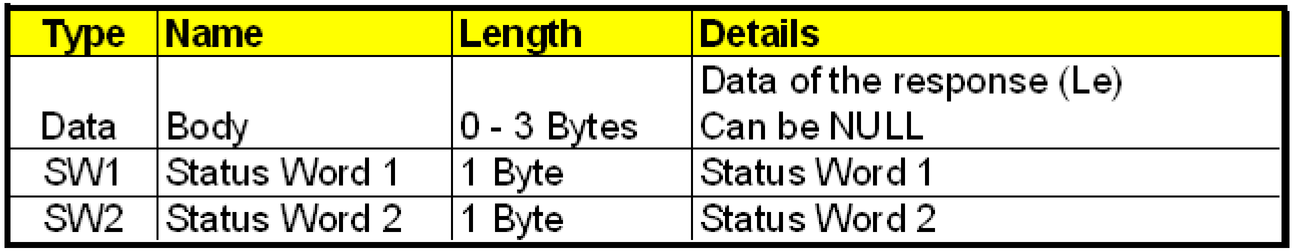


Command APDU						
CLA	INS	P1	P2	L_c	Data Field	L_e

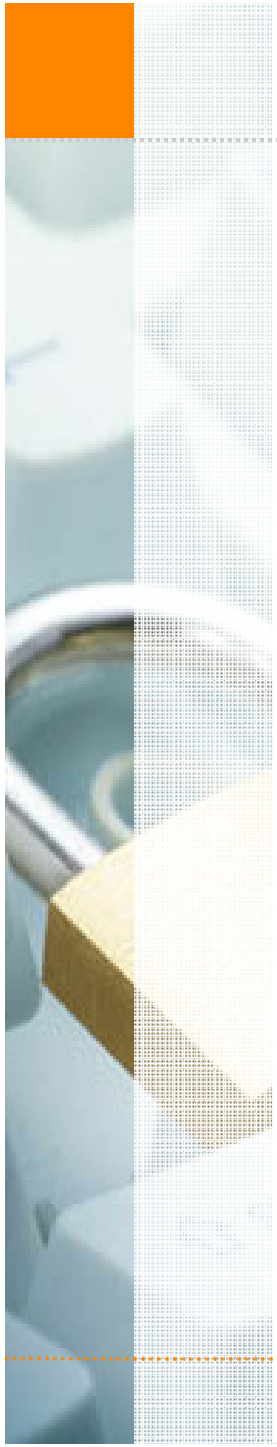


Response APDU		
Response	SW1	SW2

APDU Response Details

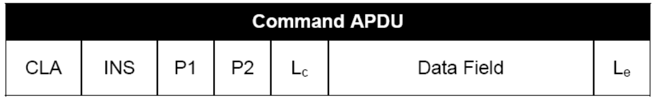


Type	Name	Length	Details
Data	Body	0 - 3 Bytes	Data of the response (Le) Can be NULL
SW1	Status Word 1	1 Byte	Status Word 1
SW2	Status Word 2	1 Byte	Status Word 2

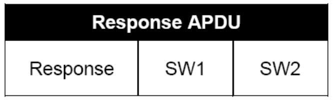


Smart Card::APDU::Enter PIN

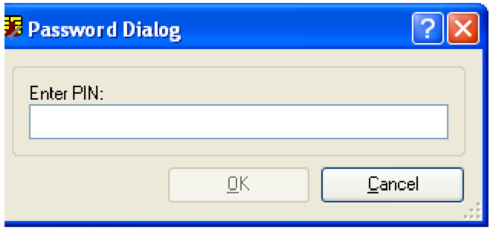
Example: APDU Enter PIN



Command APDU						
CLA	INS	P1	P2	L_c	Data Field	L_e



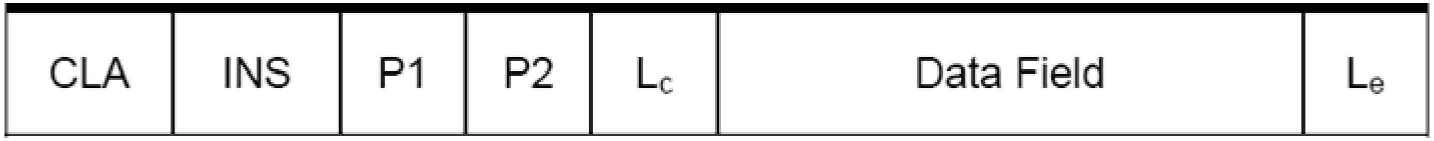
Response APDU		
Response	SW1	SW2



Enter PIN:

APDU Command

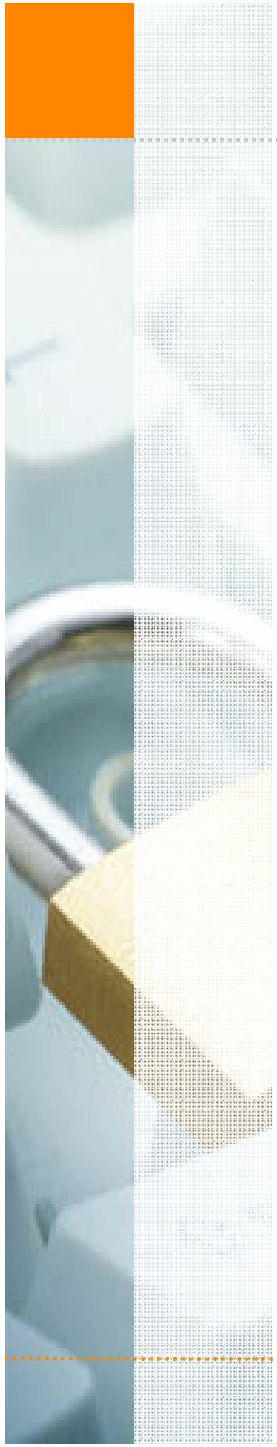
C0 20 00 01 08 303030303030303030



CLA	INS	P1	P2	L_c	Data Field	L_e

APDU Response

90 00



Smart Card::APDU::Standards

GSC-IS (Government Smart Card Interoperability Specification)

- ISO Standard (APDU)
  - 7816-4: Organization, security and commands for interchange
  - 7816-8: Commands for security operations
- Goal of GSC-IS
  - Interoperability requirements of the enterprise market

EMV - CAP

- Europay/MasterCard/Visa - Chip Authentication Program

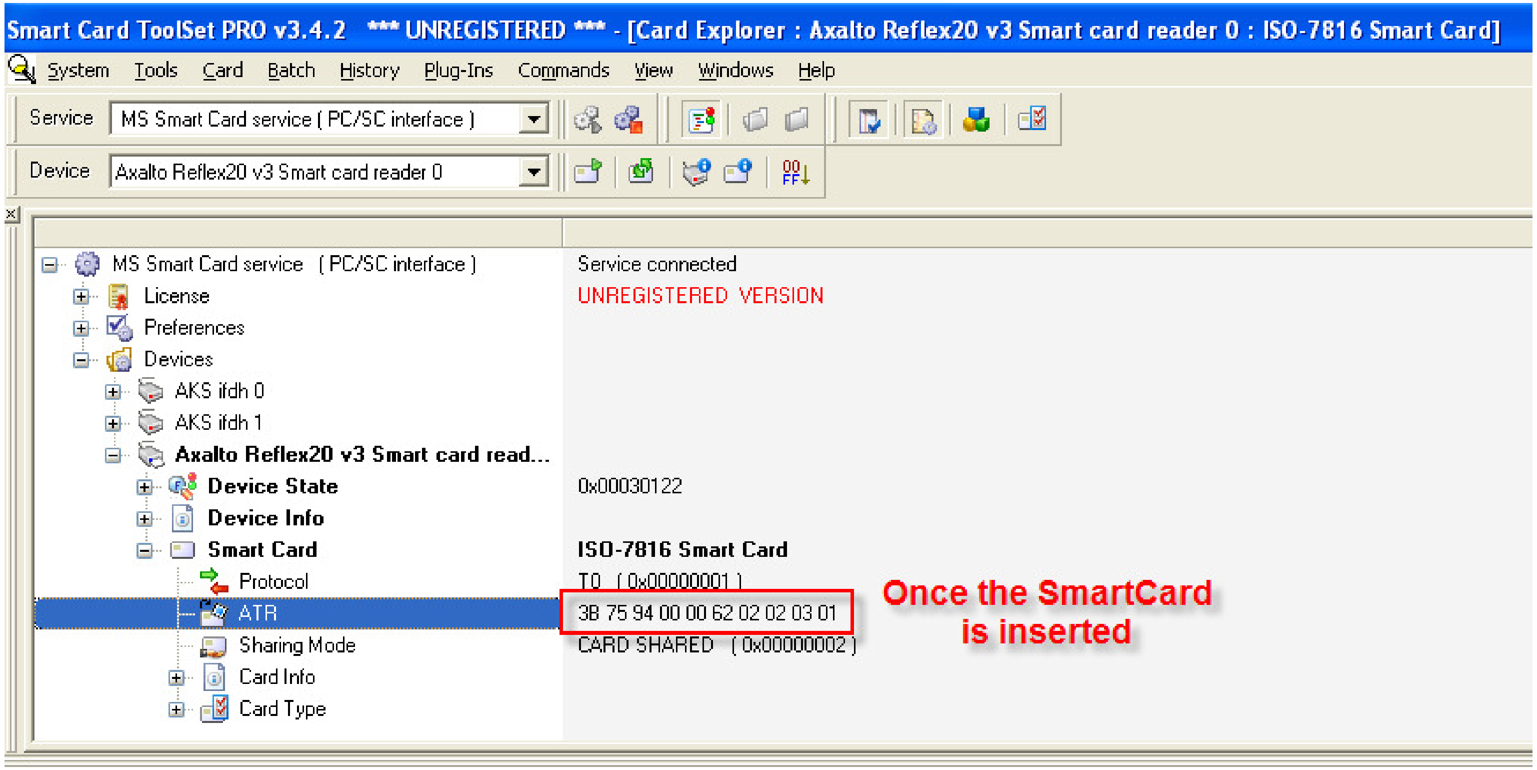
GSM (Global System Mobile)

- GSM Standard

Smart Card::ATR::Answer to Reset

ATR String: Unique Identification for Smart Cards

- ATR (Answer to Reset) returns unique number
- Unique number references to the appropriate DLL (registry key)



Smart Card ToolSet PRO v3.4.2 *** UNREGISTERED *** - [Card Explorer : Axalto Reflex20 v3 Smart card reader 0 : ISO-7816 Smart Card]

Service: MS Smart Card service (PC/SC interface)

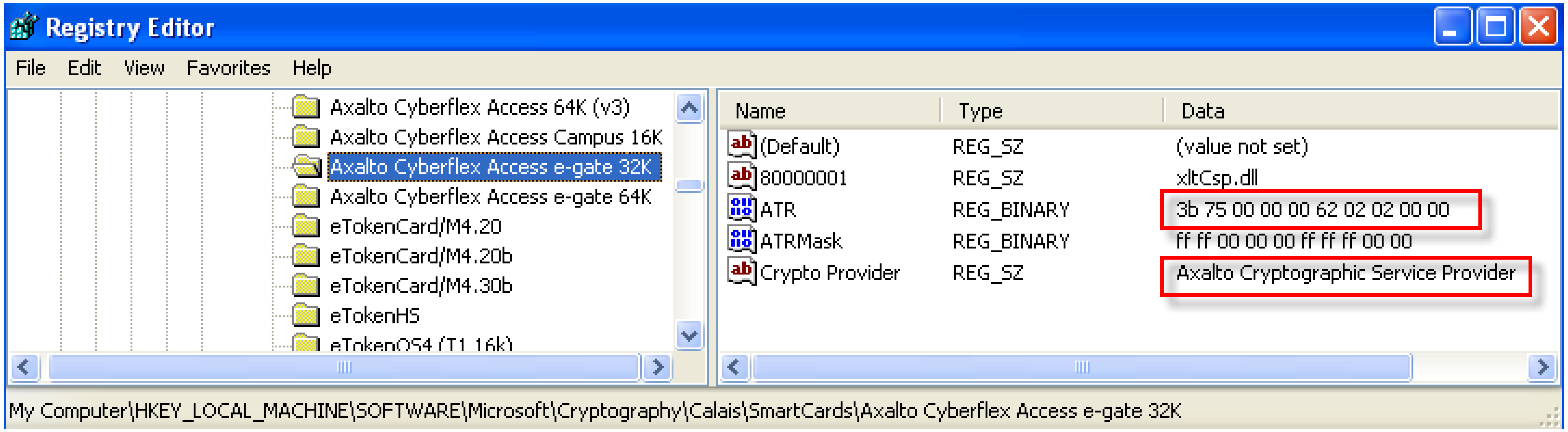
Device: Axalto Reflex20 v3 Smart card reader 0

```
MS Smart Card service  ( PC/SC interface )     Service connected
  License                                      UNREGISTERED VERSION
  Preferences
  Devices
    AKS ifdh 0
    AKS ifdh 1
    Axalto Reflex20 v3 Smart card read...
      Device State                             0x00030122
      Device Info
      Smart Card                               ISO-7816 Smart Card
        Protocol                               T0  ( 0x00000001 )
        ATR                                    3B 75 94 00 00 62 02 02 03 01
        Sharing Mode                           CARD SHARED  ( 0x00000002 )
        Card Info
        Card Type
```

Once the SmartCard is inserted

Smart Card::APDU::CSP

ATR: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\Smart Cards

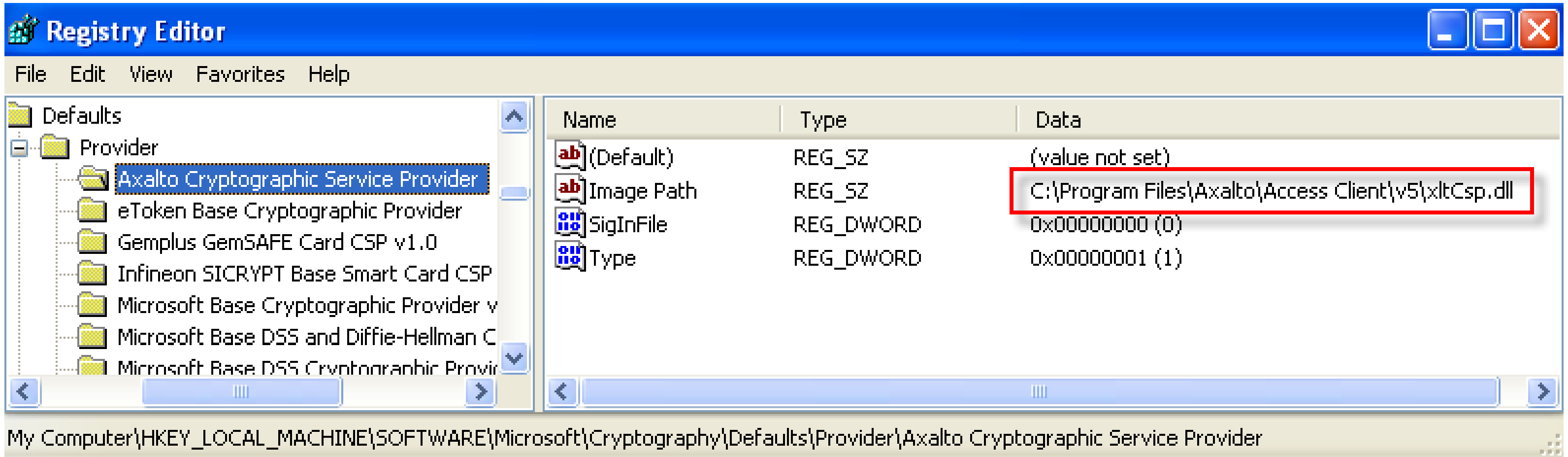


- Axalto Cyberflex Access 64K (v3)
- Axalto Cyberflex Access Campus 16K
- Axalto Cyberflex Access e-gate 32K
- Axalto Cyberflex Access e-gate 64K
- eTokenCard/M4.20
- eTokenCard/M4.20b
- eTokenCard/M4.30b
- eTokenHS
- eTokenOS4 (T1 16k)

Name	Type	Data
(Default)	REG_SZ	(value not set)
80000001	REG_SZ	xltCsp.dll
ATR	REG_BINARY	3b 75 00 00 00 62 02 02 00 00
ATRMask	REG_BINARY	ff ff 00 00 00 ff ff ff 00 00
Crypto Provider	REG_SZ	Axalto Cryptographic Service Provider

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\Axalto Cyberflex Access e-gate 32K

Service Provider: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider



- Defaults
  - Provider
    - Axalto Cryptographic Service Provider
    - eToken Base Cryptographic Provider
    - Gemplus GemSAFE Card CSP v1.0
    - Infineon SICRYPT Base Smart Card CSP
    - Microsoft Base Cryptographic Provider v
    - Microsoft Base DSS and Diffie-Hellman C
    - Microsoft Base DSS Cryptographic Provic

Name	Type	Data
(Default)	REG_SZ	(value not set)
Image Path	REG_SZ	C:\Program Files\Axalto\Access Client\v5\xltCsp.dll
SigInFile	REG_DWORD	0x00000000 (0)
Type	REG_DWORD	0x00000001 (1)

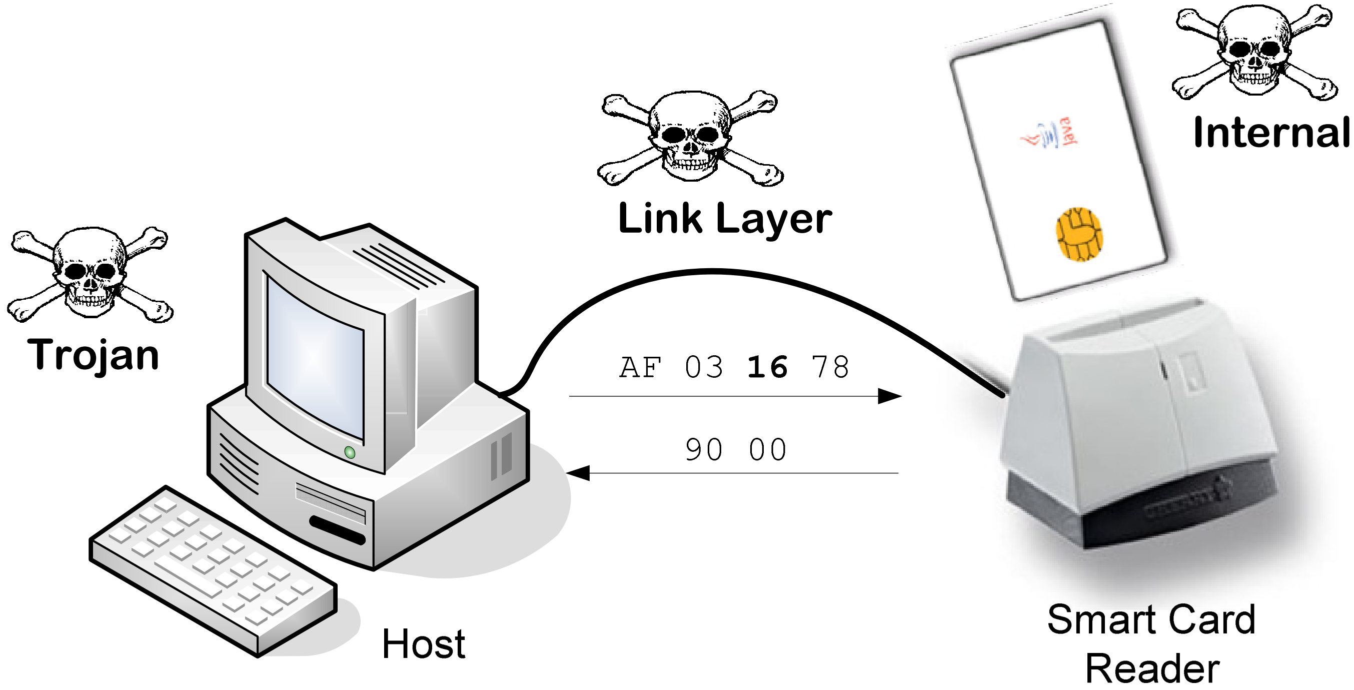
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Axalto Cryptographic Service Provider

ATTACKING Smart Card SOLUTIONS

Introduction::Smart Card Attacks

Attacking Approaches

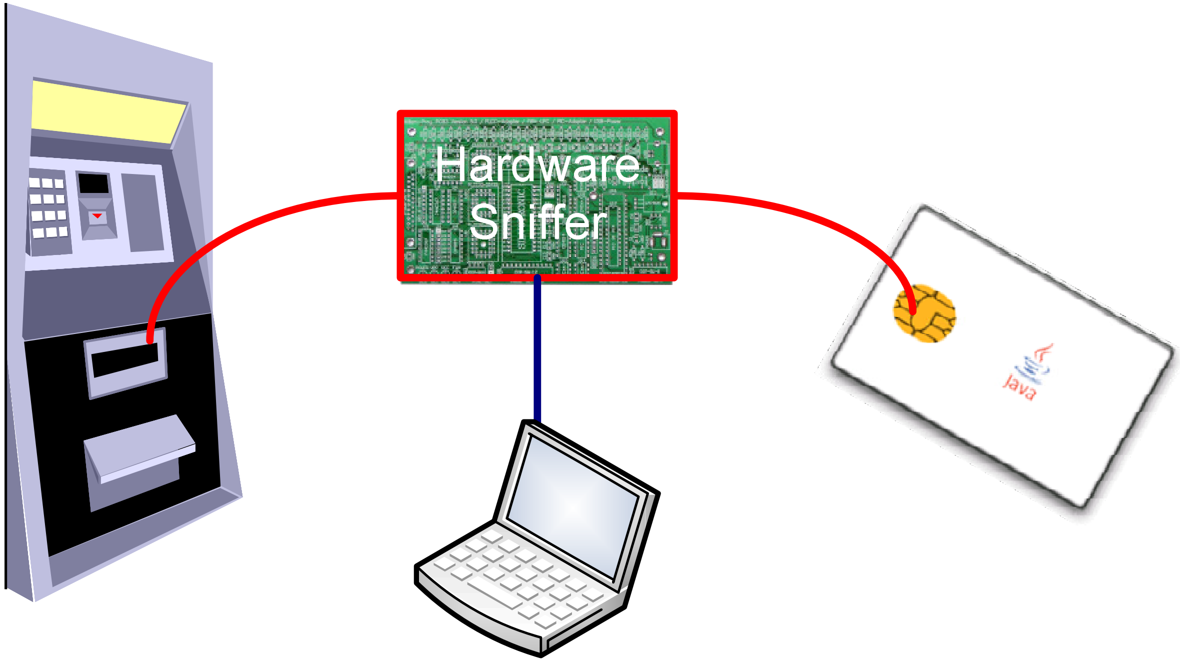
- Host Computer (Software)
- Transmission (Link Layer)
- Internal Smart Card (Physical, Side Channel Attacks, not covered here)



Hardware::Sniffing APDU

Hardware APDU Sniffing Device

- The APDU sequences are not commonly known – hidden secret disclosure
  - ATM APDU analysis
  - GSM APDU analysis

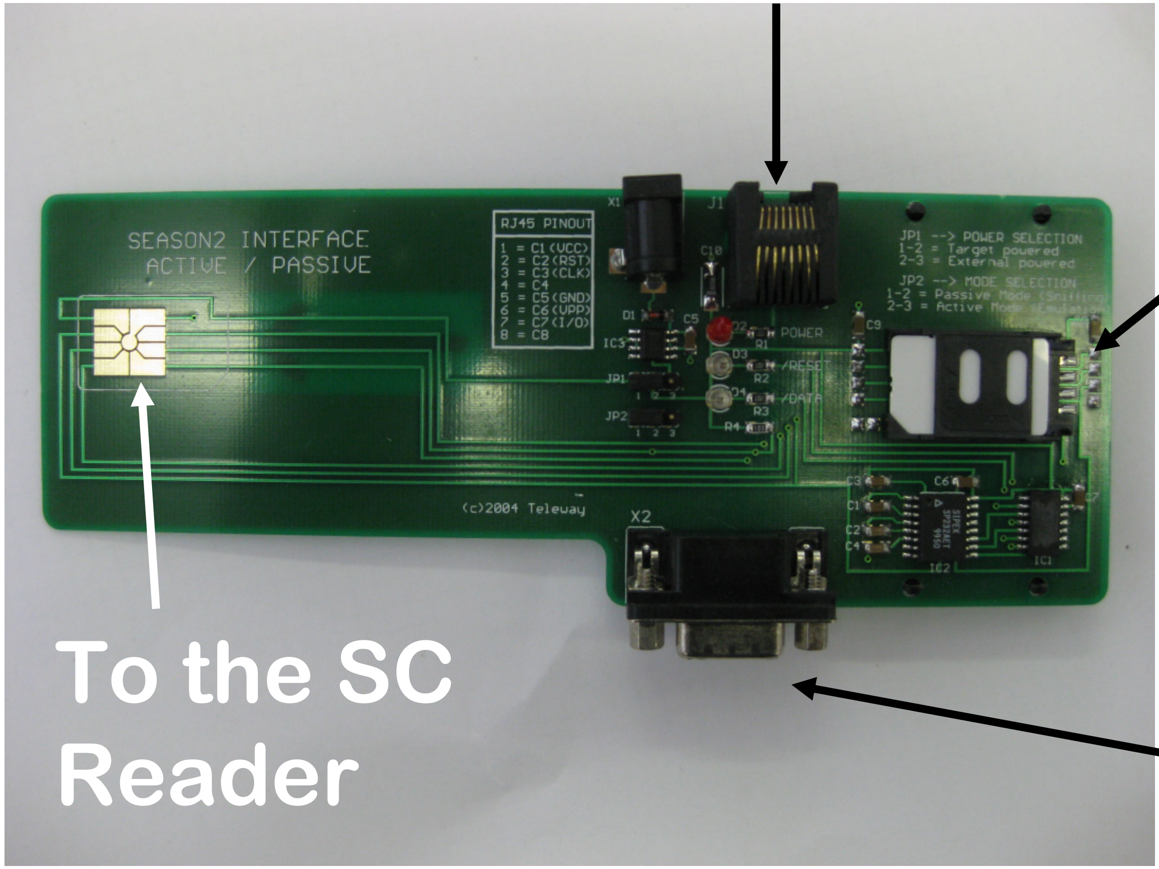


RS232
Sniffing Packets

Hardware::Sniffing APDU

Season2 Interface

To the SC Reader

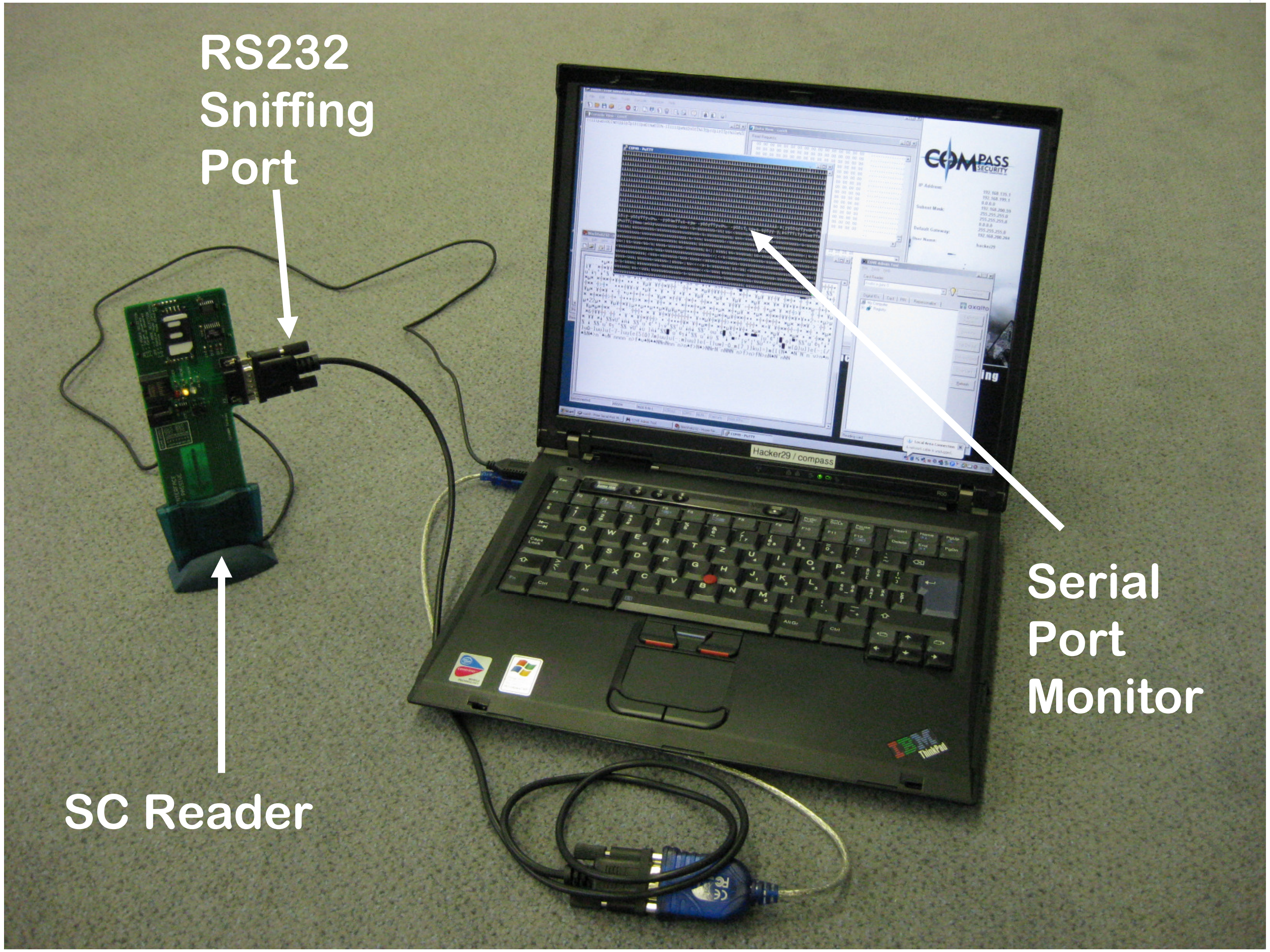


Smart Card

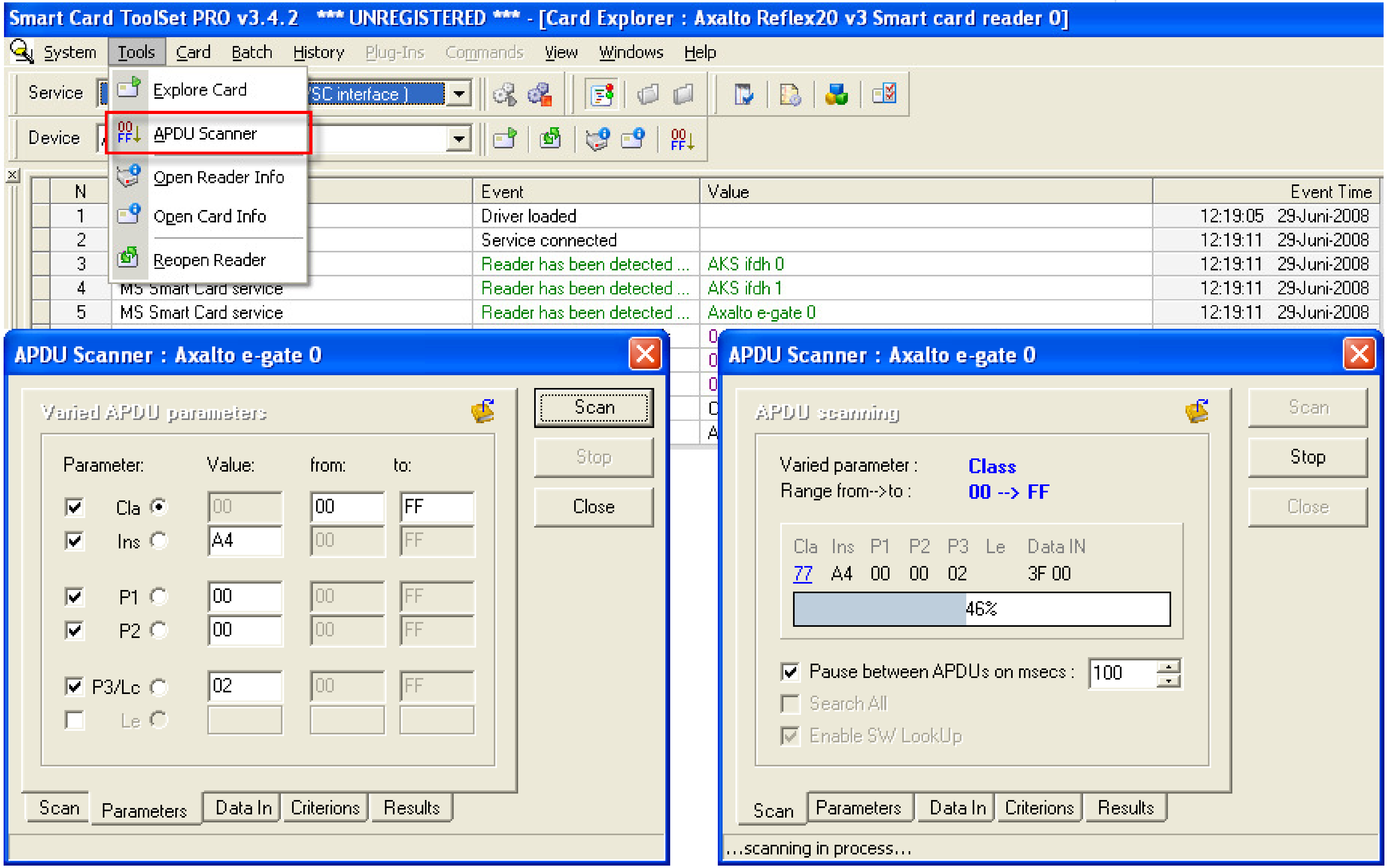
To the SC Reader

RS232 Sniffing Port

Hardware::Sniffing APDU



Software::Scanning APDU Commands



Smart Card ToolSet PRO v3.4.2 *** UNREGISTERED *** - [Card Explorer : Axalto Reflex20 v3 Smart card reader 0]

N		Event	Value	Event Time
1		Driver loaded		12:19:05 29-Juni-2008
2		Service connected		12:19:11 29-Juni-2008
3		Reader has been detected ...	AKS ifdh 0	12:19:11 29-Juni-2008
4	MS Smart Card service	Reader has been detected ...	AKS ifdh 1	12:19:11 29-Juni-2008
5	MS Smart Card service	Reader has been detected ...	Axalto e-gate 0	12:19:11 29-Juni-2008

APDU Scanner : Axalto e-gate 0

Varied APDU parameters

Parameter:		Value:	from:	to:
☑ Cla	●	00	00	FF
☑ Ins	○	A4	00	FF
☑ P1	○	00	00	FF
☑ P2	○	00	00	FF
☑ P3/Lc	○	02	00	FF
□ Le	○			

APDU Scanner : Axalto e-gate 0

APDU scanning

Varied parameter : **Class**

Range from-->to : **00 --> FF**

Cla	Ins	P1	P2	P3	Le	Data IN
77	A4	00	00	02		3F 00

46%

☑ Pause between APDUs on msecs : 100

□ Search All

☑ Enable SW LookUp

...scanning in process...

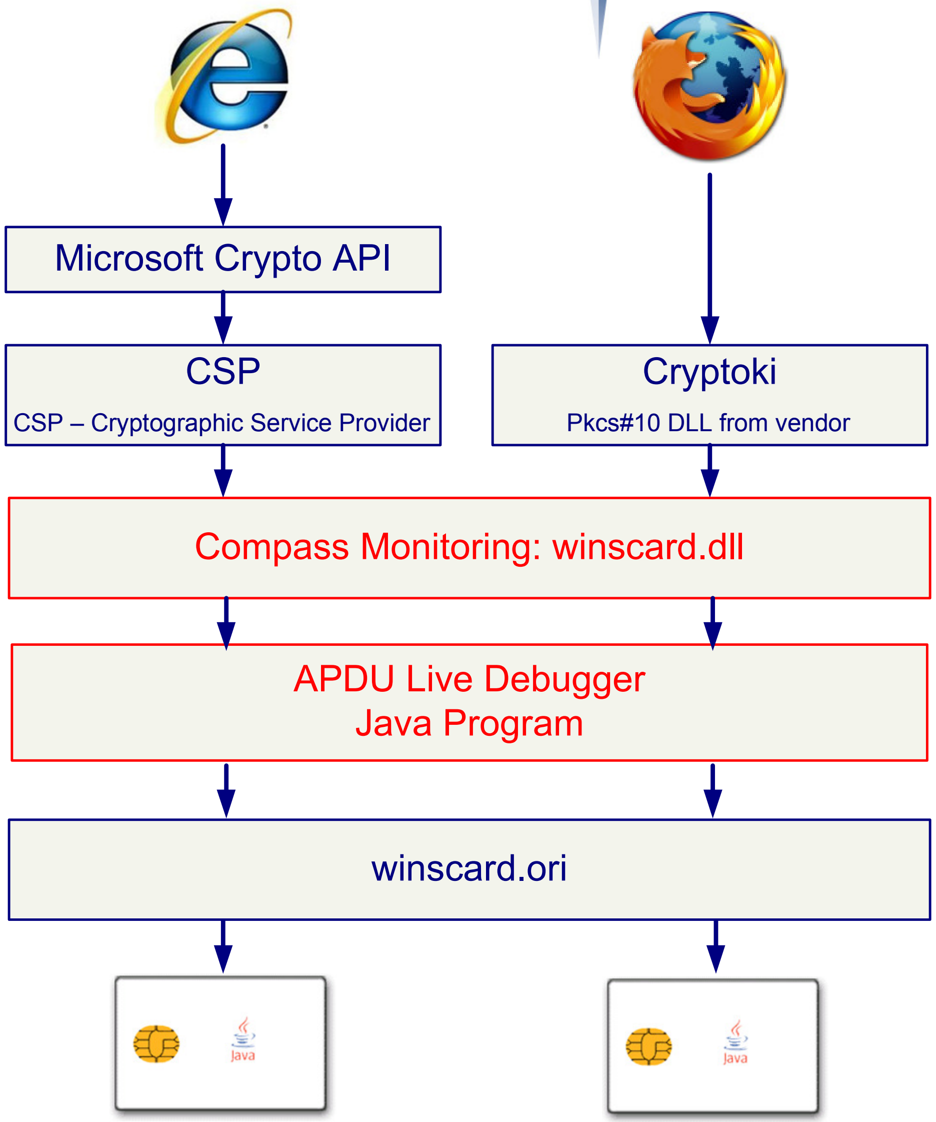
Software::APDU LiveDebugger

Live Debugger

- DLL Proxy winscard.dll
- Analyzing any software that communicates with the Smart Card with winscard.dll
- Works with PKCS#10 or CSP enabled applications

Live Debugger Features

- Command Modification
- Response Modification
- Logging



Microsoft Crypto API

CSP

CSP – Cryptographic Service Provider

Cryptoki

Pkcs#10 DLL from vendor

Compass Monitoring: winscard.dll

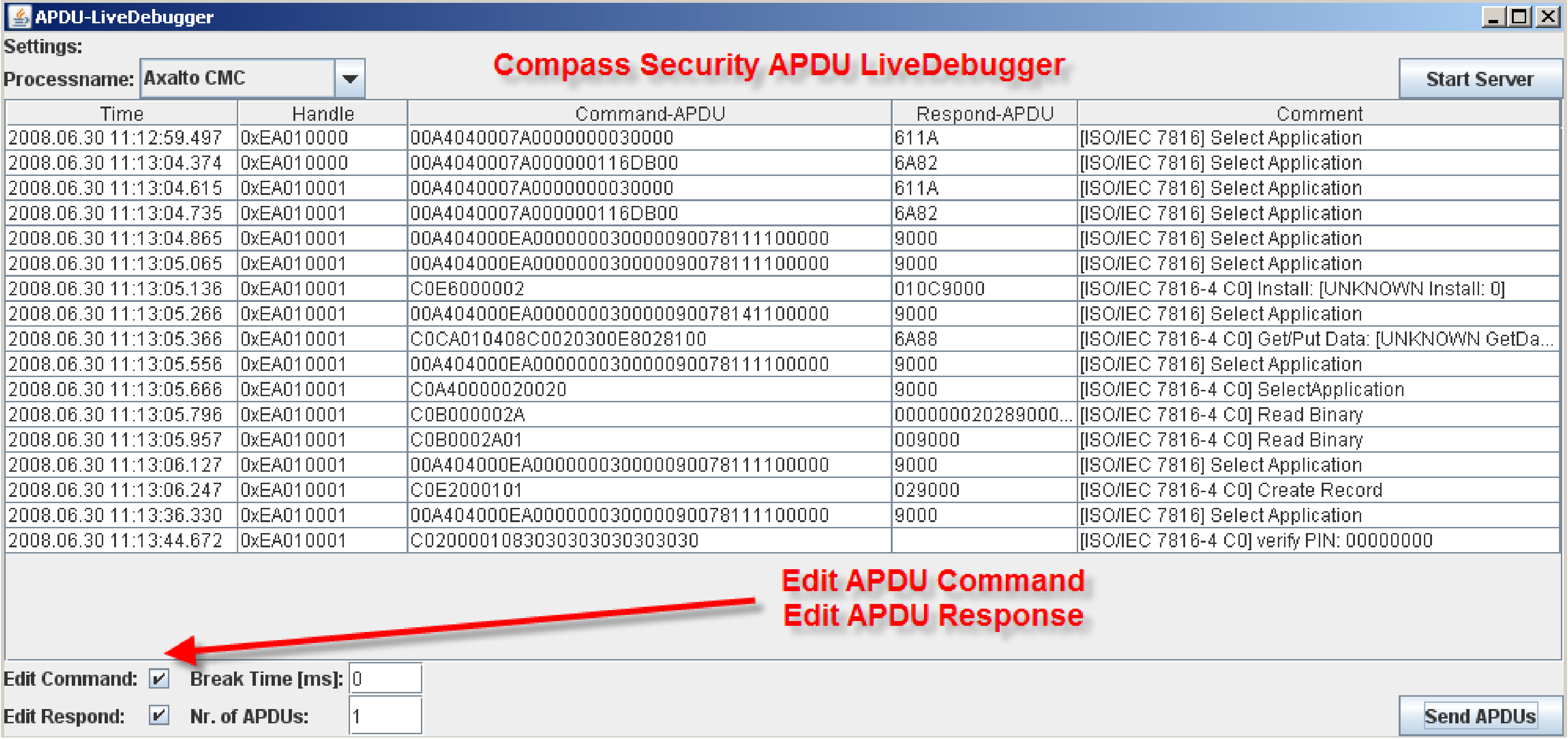
APDU Live Debugger
Java Program

winscard.ori

Software::APDU LiveDebugger

APDU Live Debugger: APDU Inspection/Interception

- Live Debugging
- Command & Response Interception



Settings:

Processname: Axalto CMC

Time	Handle	Command-APDU	Respond-APDU	Comment
2008.06.30 11:12:59.497	0xEA010000	00A4040007A0000000030000	611A	[ISO/IEC 7816] Select Application
2008.06.30 11:13:04.374	0xEA010000	00A4040007A000000116DB00	6A82	[ISO/IEC 7816] Select Application
2008.06.30 11:13:04.615	0xEA010001	00A4040007A0000000030000	611A	[ISO/IEC 7816] Select Application
2008.06.30 11:13:04.735	0xEA010001	00A4040007A000000116DB00	6A82	[ISO/IEC 7816] Select Application
2008.06.30 11:13:04.865	0xEA010001	00A404000EA000000030000090078111100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:05.065	0xEA010001	00A404000EA000000030000090078111100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:05.136	0xEA010001	C0E6000002	010C9000	[ISO/IEC 7816-4 C0] Install: [UNKNOWN Install: 0]
2008.06.30 11:13:05.266	0xEA010001	00A404000EA000000030000090078141100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:05.366	0xEA010001	C0CA010408C0020300E8028100	6A88	[ISO/IEC 7816-4 C0] Get/Put Data: [UNKNOWN GetDa...
2008.06.30 11:13:05.556	0xEA010001	00A404000EA000000030000090078111100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:05.666	0xEA010001	C0A40000020020	9000	[ISO/IEC 7816-4 C0] SelectApplication
2008.06.30 11:13:05.796	0xEA010001	C0B000002A	000000020289000...	[ISO/IEC 7816-4 C0] Read Binary
2008.06.30 11:13:05.957	0xEA010001	C0B0002A01	009000	[ISO/IEC 7816-4 C0] Read Binary
2008.06.30 11:13:06.127	0xEA010001	00A404000EA000000030000090078111100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:06.247	0xEA010001	C0E2000101	029000	[ISO/IEC 7816-4 C0] Create Record
2008.06.30 11:13:36.330	0xEA010001	00A404000EA000000030000090078111100000	9000	[ISO/IEC 7816] Select Application
2008.06.30 11:13:44.672	0xEA010001	C02000010830303030303030		[ISO/IEC 7816-4 C0] verify PIN: 00000000

Edit Command: ☑ Break Time [ms]: 0

Edit Respond: ☑ Nr. of APDUs: 1

APDU LiveDebugger Discovery!

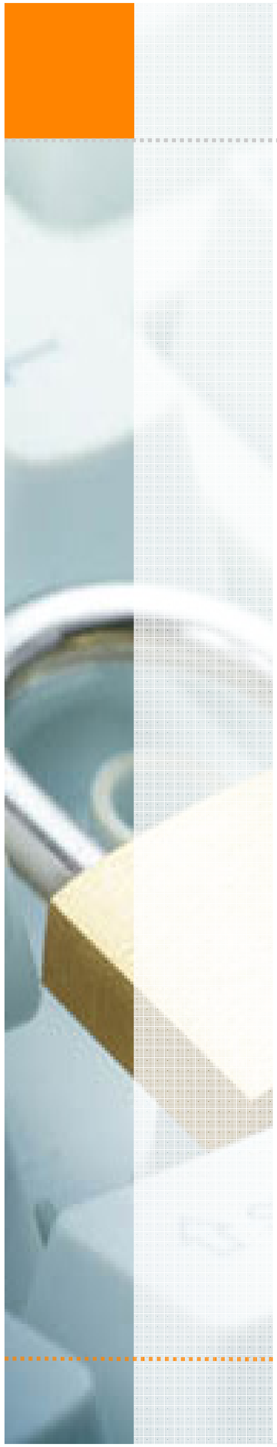
APDU::LiveDebugger::Results

APDU Control Sequences

```
80 XX XX XX Not encrypted (Axalto Commands)
84 XX XX XX Encrypted
C0 XX XX XX Not encrypted
00 XX XX XX ISO Standard APDU
```

APDU Instructions

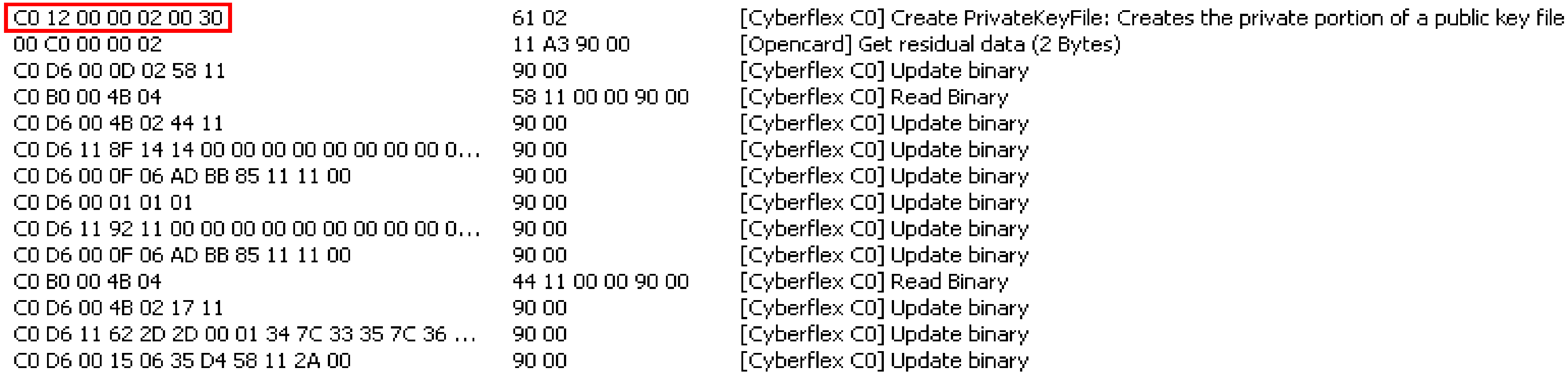
```
XX B0 XX XX Read
XX D6 XX XX Write
C0 D2 XX XX Generate keys on Smart Card
C0 12 XX XX Generate keys on PC
XX A4 XX XX Select Instance
```



APDU::LiveDebugger::Results

C0 12: Generate Keys on Computer (not on Smart Card)

- First: Offcard key generation
- Then: Storing keys onto the Smart Card

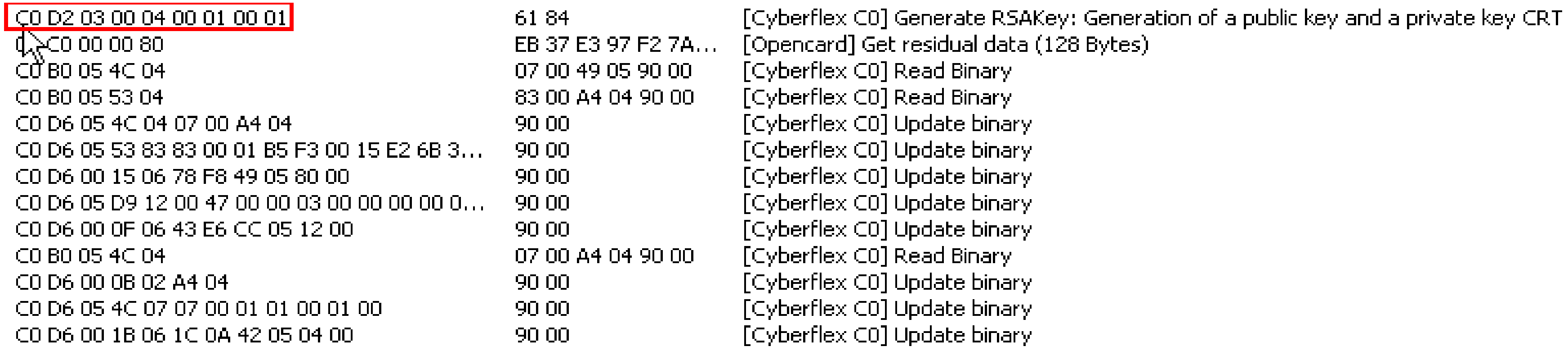


```
C0 12 00 00 02 00 30                          61 02              [Cyberflex C0] Create PrivateKeyFile: Creates the private portion of a public key file
00 C0 00 00 02                                11 A3 90 00        [Opencard] Get residual data (2 Bytes)
C0 D6 00 0D 02 58 11                          90 00              [Cyberflex C0] Update binary
C0 B0 00 4B 04                                58 11 00 00 90 00  [Cyberflex C0] Read Binary
C0 D6 00 4B 02 44 11                          90 00              [Cyberflex C0] Update binary
C0 D6 11 8F 14 14 00 00 00 00 00 00 00 00 0...  90 00            [Cyberflex C0] Update binary
C0 D6 00 0F 06 AD BB 85 11 11 00              90 00              [Cyberflex C0] Update binary
C0 D6 00 01 01 01                             90 00              [Cyberflex C0] Update binary
C0 D6 11 92 11 00 00 00 00 00 00 00 00 00 0...  90 00            [Cyberflex C0] Update binary
C0 D6 00 0F 06 AD BB 85 11 11 00              90 00              [Cyberflex C0] Update binary
C0 B0 00 4B 04                                44 11 00 00 90 00  [Cyberflex C0] Read Binary
C0 D6 00 4B 02 17 11                          90 00              [Cyberflex C0] Update binary
C0 D6 11 62 2D 2D 00 01 34 7C 33 35 7C 36 ...  90 00             [Cyberflex C0] Update binary
C0 D6 00 15 06 35 D4 58 11 2A 00              90 00              [Cyberflex C0] Update binary
```

APDU::LiveDebugger::Results

C0 D2: Generate Keys on Card

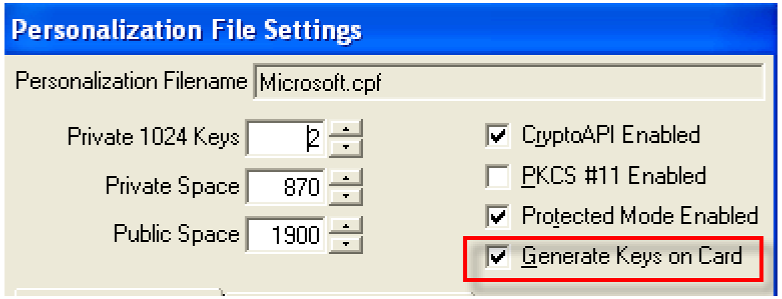
- First: Oncard key generation
- Then: Smart Card generates keys on card



```
C0 D2 03 00 04 00 01 00 01                          61 84               [Cyberflex C0] Generate RSAKey: Generation of a public key and a private key CRT
C0 C0 00 00 80                                      EB 37 E3 97 F2 7A...  [Opencard] Get residual data (128 Bytes)
C0 B0 05 4C 04                                      07 00 49 05 90 00   [Cyberflex C0] Read Binary
C0 B0 05 53 04                                      83 00 A4 04 90 00   [Cyberflex C0] Read Binary
C0 D6 05 4C 04 07 00 A4 04                          90 00               [Cyberflex C0] Update binary
C0 D6 05 53 83 83 00 01 B5 F3 00 15 E2 6B 3...      90 00               [Cyberflex C0] Update binary
C0 D6 00 15 06 78 F8 49 05 80 00                    90 00               [Cyberflex C0] Update binary
C0 D6 05 D9 12 00 47 00 00 03 00 00 00 00 0...      90 00               [Cyberflex C0] Update binary
C0 D6 00 0F 06 43 E6 CC 05 12 00                    90 00               [Cyberflex C0] Update binary
C0 B0 05 4C 04                                      07 00 A4 04 90 00   [Cyberflex C0] Read Binary
C0 D6 00 0B 02 A4 04                                90 00               [Cyberflex C0] Update binary
C0 D6 05 4C 07 07 00 01 01 00 01 00                 90 00               [Cyberflex C0] Update binary
C0 D6 00 1B 06 1C 0A 42 05 04 00                    90 00               [Cyberflex C0] Update binary
```

APDU::LiveDebugger::Results

The flag „Generate Keys on Card" is not enforced



Personalization File Settings

Personalization Filename: Microsoft.cpf

Private 1024 Keys: 2

Private Space: 870

Public Space: 1900

☑ CryptoAPI Enabled

□ PKCS #11 Enabled

☑ Protected Mode Enabled

☑ Generate Keys on Card

This results in the following attack vector

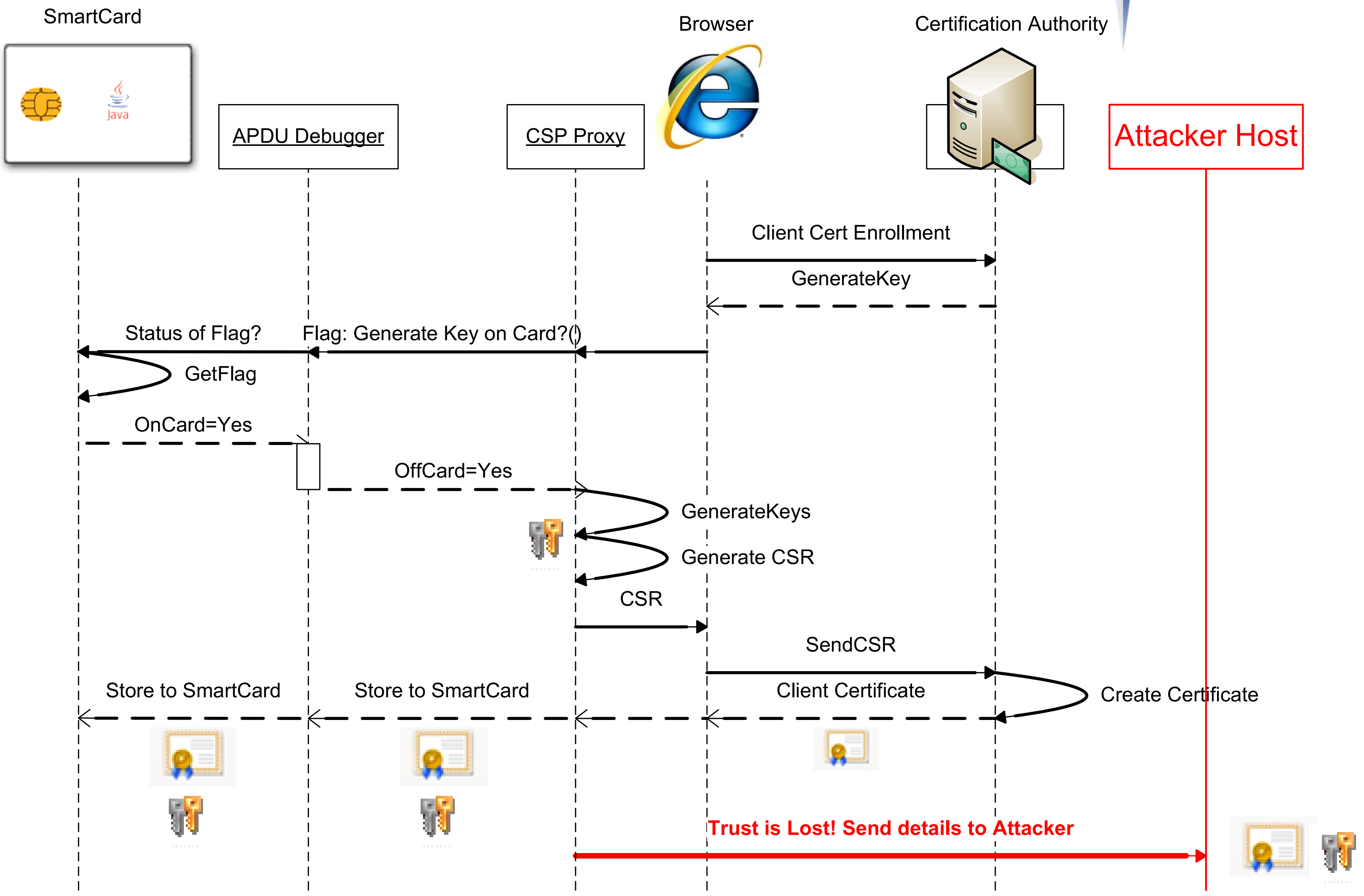
- The CSP asks the card for oncard, or offcard key generation because the card itself knows the status
- The APDU interceptor responds: „I am an offcard keygen Smart Card"
- The CSP will then perform the generate key functions on the computer
- The CSP will send the CSR to the CA
- After all, the certificate and key material will be stored onto the Smart Card
- The hacker who did all the man in the middle stuff „knows" all the keying and certificate details! **Trust is lost!**

PoC
Smart Card APDU
Attack

Compass Security AG
Glärnischstrasse 7
Postfach 1628
CH-8640 Rapperswil

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Smart Card Man-in-the-Middle Attack



Smart Card Man-in-the-Middle Attack

Conclusion

- The use of Smart Cards does not make you independent from the host computer in any case and situation!
- The flag „Generate Keys on Card“ does still allow key material being stored onto the Smart Card.
- This demonstration was solely related to Smart Cards an end-user has. If the attacker has some sort of virus/trojan running where the Smart Cards are initialized, even more fraud can occur (MasterKeySet attacks, Rogue Applet Uploads, ...)
- The PIN has been seen in plain-text within the memory segment of the Smart Card software. The PIN can be gathered without administrative privileges. By knowing the PIN, the Smart Card could be used behind the scenes without the users knowledge (signing, encryption).

Thank you!

Questions?

- ivan.buetler@csnc.ch

See you at the Swiss Cyber Storm II – Switzerland - 2009

- www.hacking-lab.com