Analysis Experience of the suspended EID Card
對「被暫停」的晶片身分證之分析經驗分享

Speaker : Shi-Cho Cha

主講人：查士朝

Dept. of Information Management, NTUST, Chairman and Professor

國立臺灣科技大學資訊管理系 教授兼系主任

Taiwan Information Security Center, Director

國立臺灣科技大學資通安全研究與教學中心主任

Background
背景

https://www.ris.gov.tw/apply-idCard/app/idcard/IDCardReissue/main

https://www.ris.gov.tw/app/portal/789

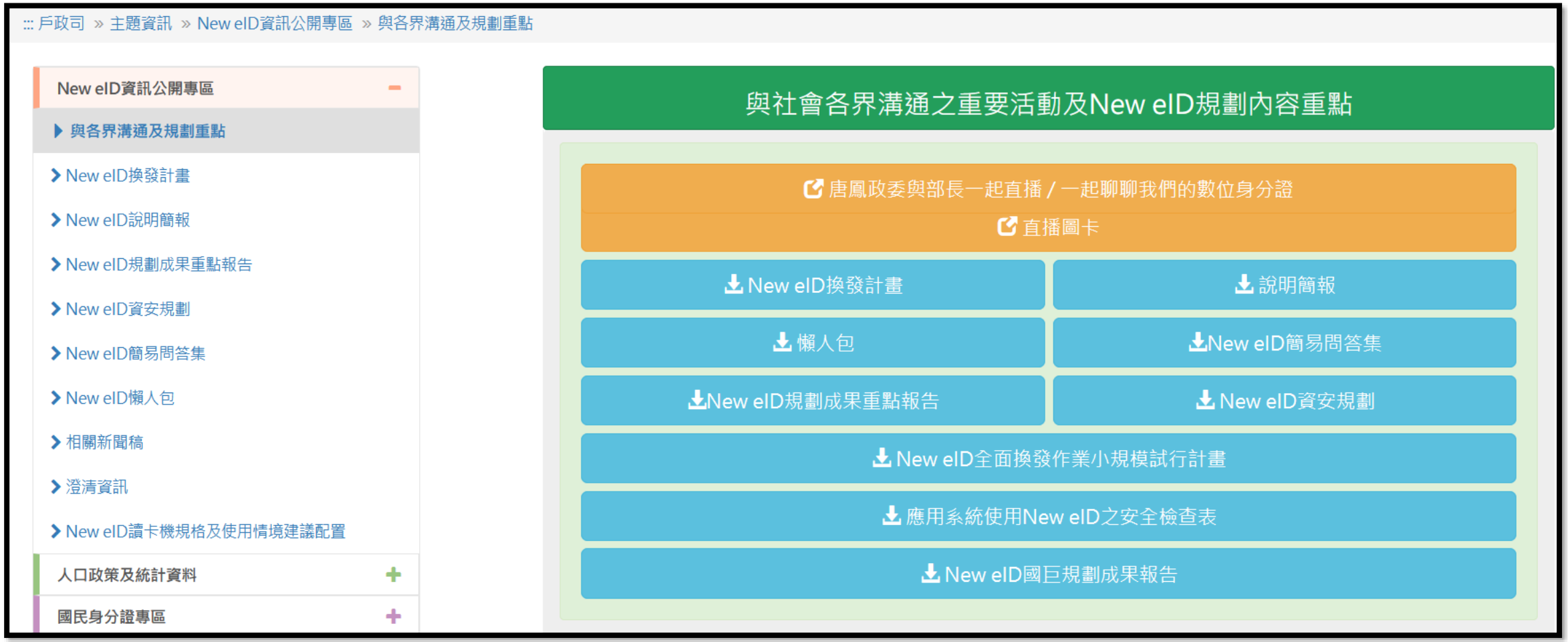
Current Status: Suspended
現況： 暫停中

https://www.ithome.com.tw/news/142375

Outline
大綱


Information Collection
資訊收集
Learning How it Works?
確認運作方式
Identifying Potential Vulnerabilities
識別可能弱點
Key Findings
主要發現
Recommendation
建議

Information Collection
資訊收集



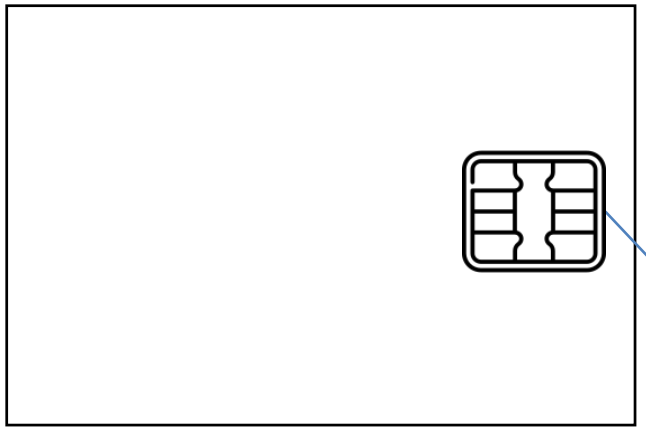
https://www.ris.gov.tw/app/portal/789

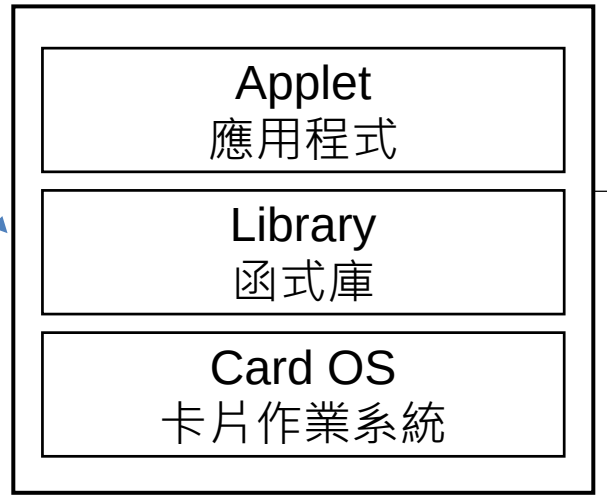
內政部

新一代國民身分證換發規劃案

規劃成果重點報告

中華民國 109 年 11 月





ISO/IEC 7816
ISO/IEC 14443

ISO 7816-4
ICAO 9303

Household Registration Address Zone
戶籍地址區

Public Data Zone
公開區

Encrypted Data Zone
加密區

Citizen Digital Certificate Zone
自然人憑證區

Common Criteria
共通準則認證

Hardware Architecture 硬體架構	Crypto. Library 密碼學函式庫	Card OS 作業系統	Applet 應用程式 EAC+SAC
EAL6+	EAL6+	EAL6+	EAL5+

Household Registration Address Zone **戶籍地區**
Household Registration Address (Village and Neighborhood) 戶籍地址 (到村里鄰)
Public Data Zone **公開區**
Name 姓名 National ID No. 統一編號 Birthday 出生日期 Household Registration Address 戶籍地址 Compulsory Military Service Status役別 Marriage Status 結婚狀態 Card ID No. 證件號碼 Date of Replacement 應換領日期 Date of Issue 製證日期 Photo 相片 (300dpi)

No Access Control 無存取控制	Contact 接觸式	Contactless 非接觸式
	○	○

ICAO SAC (Supplemental Access Control) with MRZ or CAN	Contact 接觸式	Contactless 非接觸式
	○	○

Encrypted Data Zone **加密區**
Spouse Name 配偶姓名 Father 父姓名 Mother 母姓名 Place of Birth 出生地 Gender 性別
Citizen Digital Certificate Zone **自然人憑證區**
姓名 統一編號後 4 碼 憑證序號 憑證有效日期

ICAO EAC (Extended Access Control) + TA +PIN1	Contact 接觸式	Contactless 非接觸式
	○	

PIN2	Contact 接觸式	Contactless 非接觸式
	○	

ICAO Doc 9303

- Machine Readable Travel Documents Eighth Edition, 2021
  - Part 1: Introduction
  - Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs
  - Part 3: Specifications Common to all MRTDs
  - Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs
  - Part 5: Specifications for TD1 Size Machine Readable Official Travel Documents (MROTDs)
  - Part 6: Specifications for TD2 Size Machine Readable Official Travel Documents (MROTDs)
  - Part 7: Machine Readable Visas
  - Part 8: Emergency Travel Documents
  - Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs
  - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)
  - Part 11: Security Mechanisms for MRTDs
  - Part 12: Public Key Infrastructure for MRTDs
  - Part 13: Visible Digital Seals

TD1

TD2

TD3

https://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-20/TagMrtd-20_Pres_TD-1_Broekhaar-wp20.pdf

Visa

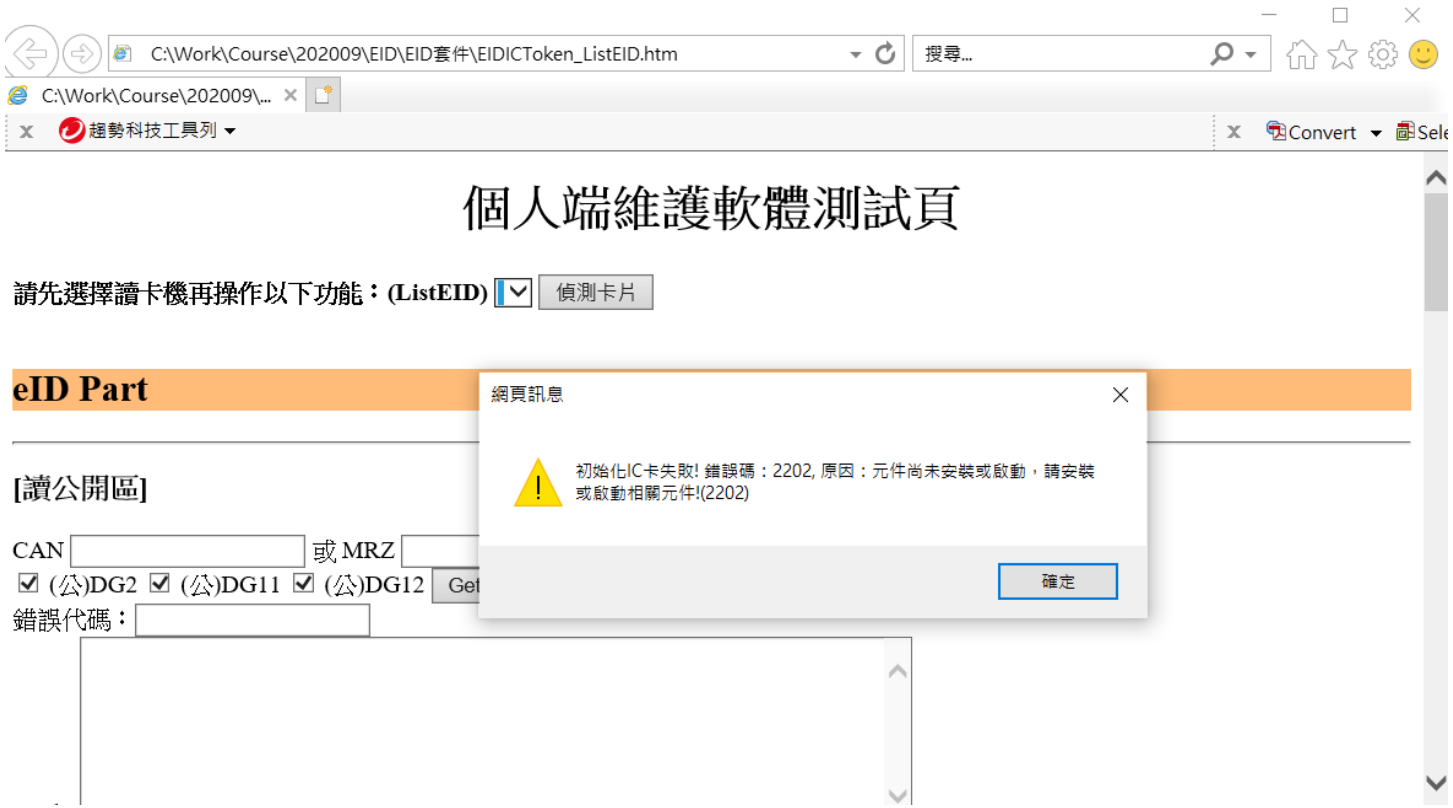
By Bundesrepublik Deutschland, Bundesministerium des Innern. - PRADO, Public Domain, https://commons.wikimedia.org/w/index.php?curid=80366059

Visa with Digital Seal

https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf

Learning How it Works?
確認運作方式

Additional HiCOS Aplication is Required
這邊需要另外裝一個 HiCOS 套件


C:\Work\Course\202009\EID\EID套件\EIDICToken_ListEID.htm
搜尋...
C:\Work\Course\202009\...
趨勢科技工具列
Convert
個人端維護軟體測試頁
請先選擇讀卡機再操作以下功能：(ListEID)
偵測卡片
eID Part
[讀公開區]
CAN
或 MRZ
(公)DG2
(公)DG11
(公)DG12
Get
錯誤代碼：
網頁訊息
初始化IC卡失敗! 錯誤碼：2202, 原因：元件尚未安裝或啟動，請安裝或啟動相關元件!(2202)
確定


頁面載入發生問題 — Mozilla Firefox
localhost:61161/eIDPM/ChtPopupFormEIDPM
連線失敗
Firefox 無法與伺服器 localhost:61161 建立連線。
該網站可能暫時無法使用或太過忙碌，請過幾分鐘後再試試。
若無法載入任何網站，請檢查您的網路連線狀態。
若電腦或網路被防火牆或 Proxy 保護，請確定 Firefox 被允許存取網路。

result:

eidRawdata:

[讀戶籍區]

GetEIDHouseholdData

錯誤代碼：0

result:
```
戶籍地址(到村里):65000120005
戶籍地址(鄰):010
戶籍地址(到村里鄰):新北市,瑞芳區龍山里,010鄰
```

You can read the Household Registration Address Zone Directly
可以直接讀戶籍地址區

[讀公開區]

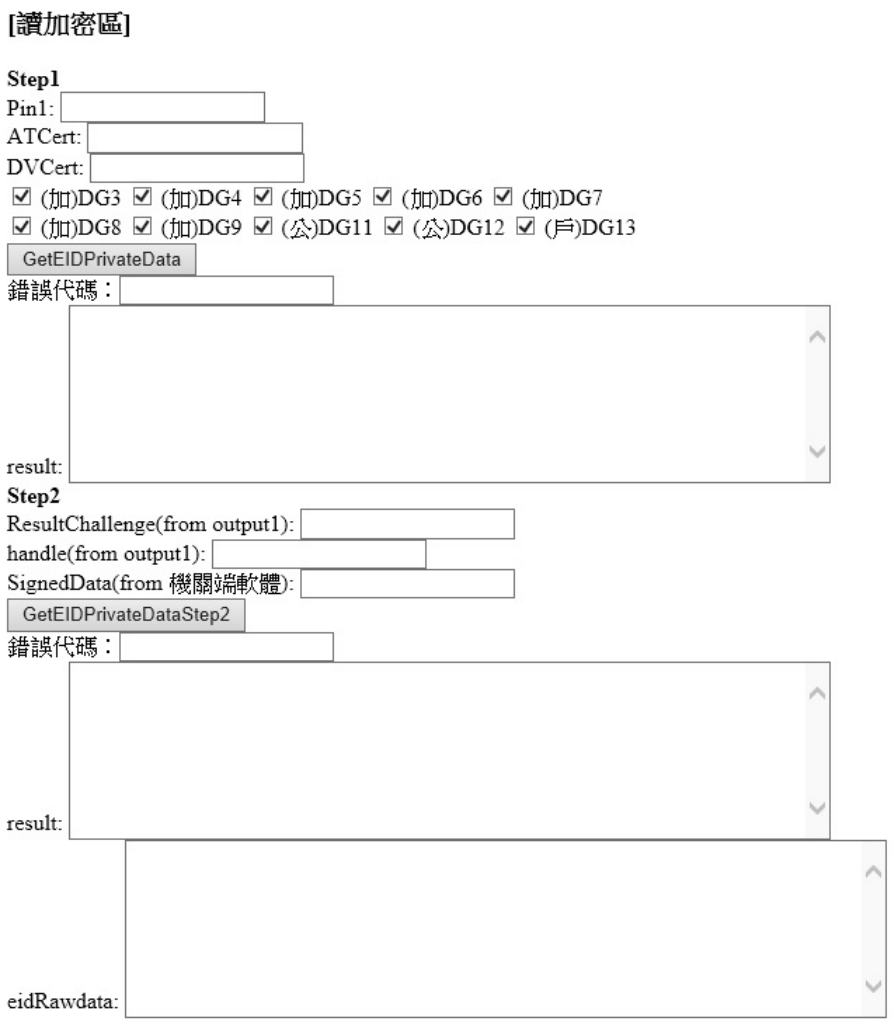
CAN 000005 或 MRZ 或 證件號碼
☑ (公)DG2 ☑ (公)DG11 ☑ (公)DG12 GetEIDPublicData
錯誤代碼：0

result:
```
證件號碼:AT0000005
應換領日期(西元):20301015
製證日期(西元):20201015
驗證資訊:1000901952100239
姓名羅馬拼音:
役別:
戶籍地址:新北市瑞芳區龍山里010鄰逢甲路２８０號
```

eidRawdata:

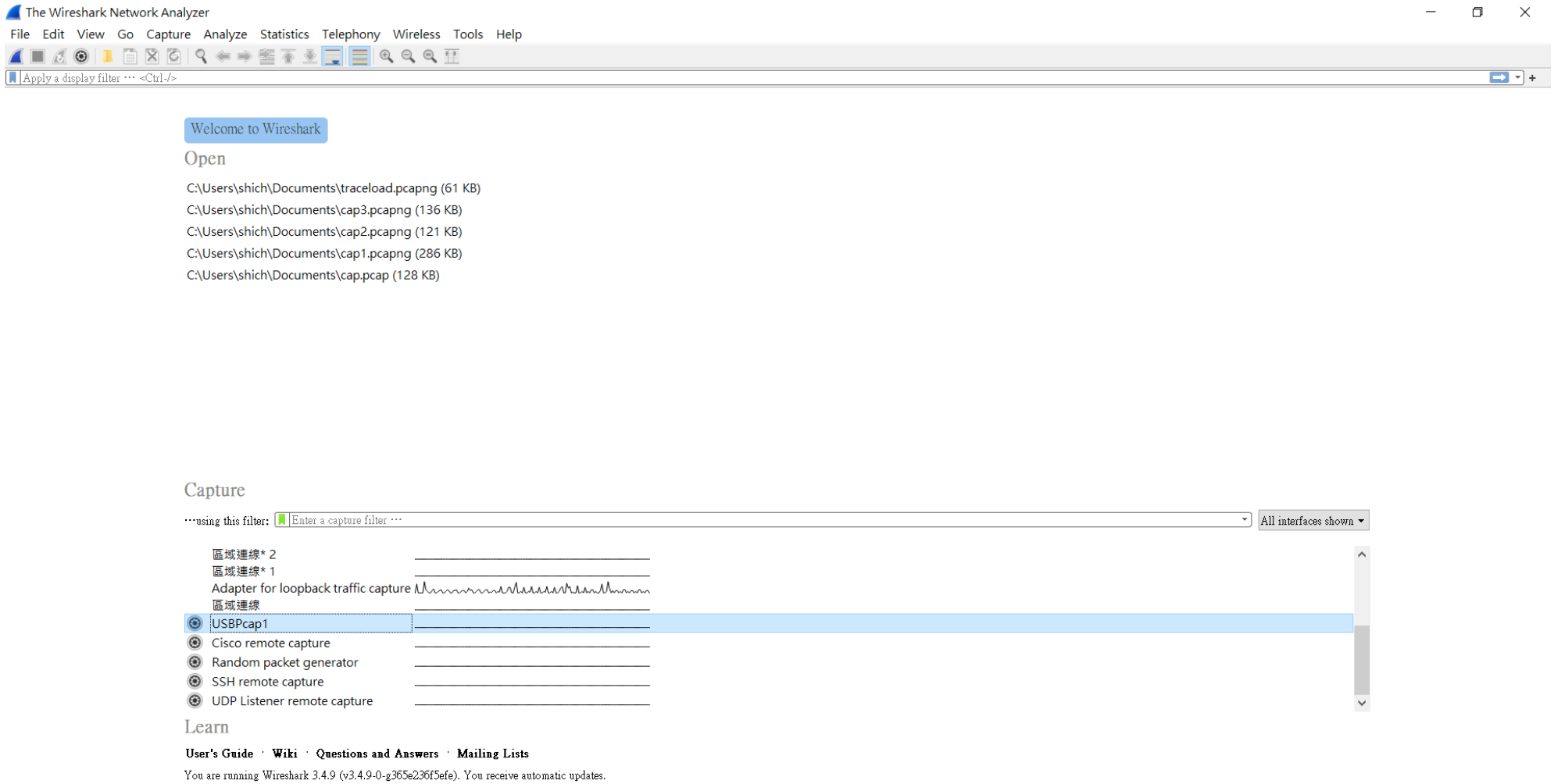
```
{"sod":"d4IGuzCCBrcGCSqGSIb3DQEHAqCCBqgwggakAgEDMQ8wDQYJYIZIAWUDB
AIBBQAwggIOBgZngQgBAQGgggICBIIB/jCCAfoCAQEwDQYJYIZIAWUDBAIBBQAwgg
HUMCUCAQIEINxzQlsfNt73ltMpZKXzza90N/mii8F0RrDnwH4Iz092MCUCAQMEIC/
8jIWTiGvqbehN8m0/oxlOlwtb1UlskXc90Ir6Qrk+MCUCAQQEIPx8uHRKbuF2t5IV
cR22r8y318Iv5MeCU8phsPH8xd2tMCUCAQUEIL8rWx9jlsrnLLd25AZSFYHgj7jAc
FkBjw1C7GpWQUiOMCUCAQYEIB6H7vxOPy9DQ5x2iur+zjnls0kQD6bErEJwEMa1lo
1ZMCUCAQcEIOrzjhDrd2t+deO6Qym+w74PcsLC79JwKqCuzTMhs0EJMCUCAQgEIGf
XIgnY3tvdOAM7ltVj3eeSERUc5iG+FlyuHVjtGbseMCUCAQkEIDRR3KdVIjBpNQk5
```


You need MRZ or CAN to Read the Public Data Zone
需要使用 MRZ 或 CAN 以讀取公開區



It is Very Complicated to Read the Encrypted Data Zone
要讀取加密區就複雜了 ……

Capture the USB Packets with Wireshark and USBPCap
可以使用 Wireshark 與 USBPCap 去抓取 USB 封包



Test Standard is Good Resource
測試標準是可以讓我們了解正常運作方式的最佳資源

For Publication on the ICAO Website

TECHNICAL REPORT

Radio Frequency Protocol and Application Test Standard for eMRTD – Part 3

Tests for Application Protocol and Logical Data Structure

Version 2.11

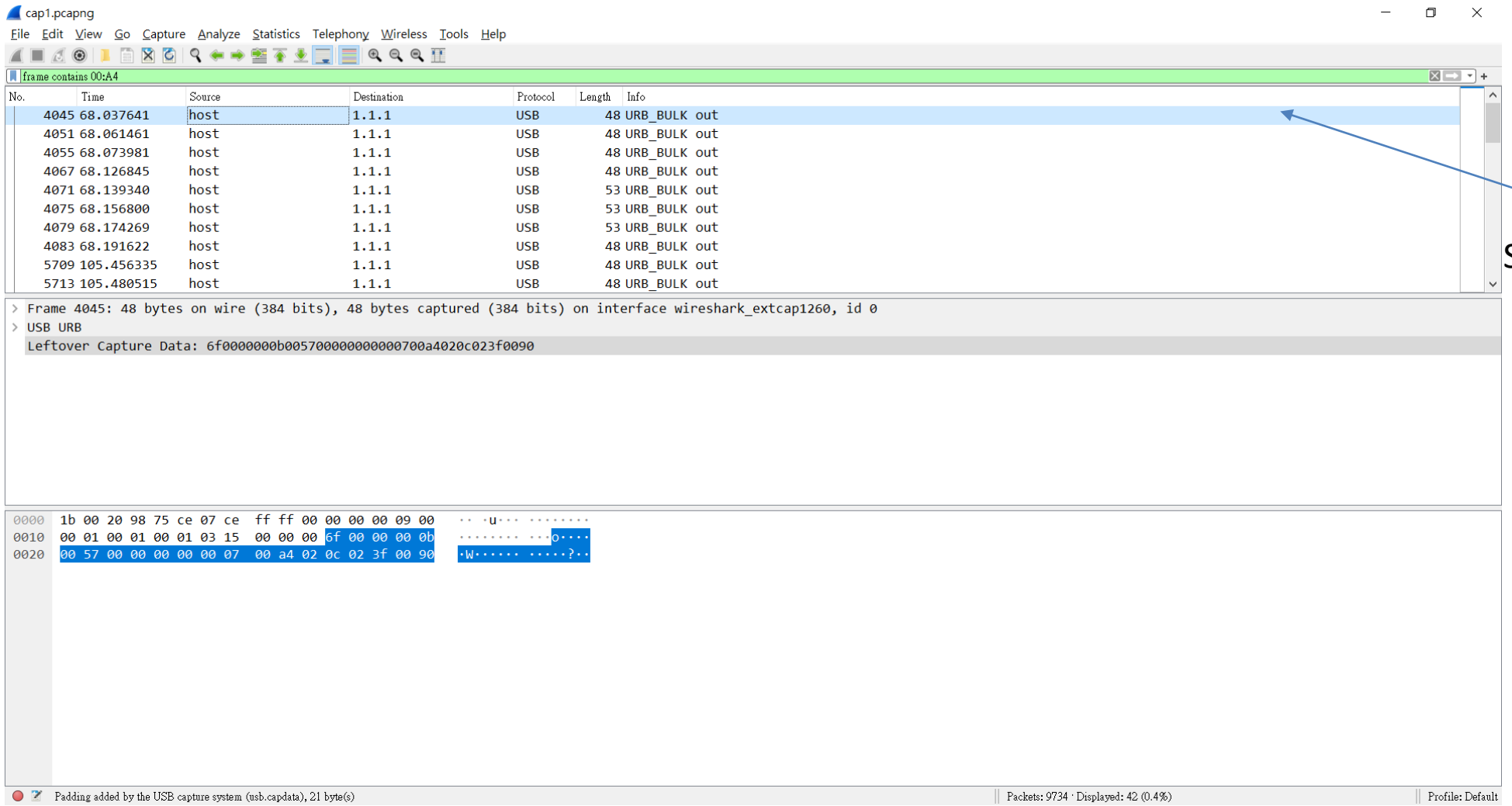
March 2018

File: Technical Report - Radio Frequency and Protocol Testing Part 3 V2.11.docx
Author: ISO/JTC1/SC17/WG3/TF4 for ICAO-NTWG

3.1.2 Test Case ISO7816_A_2

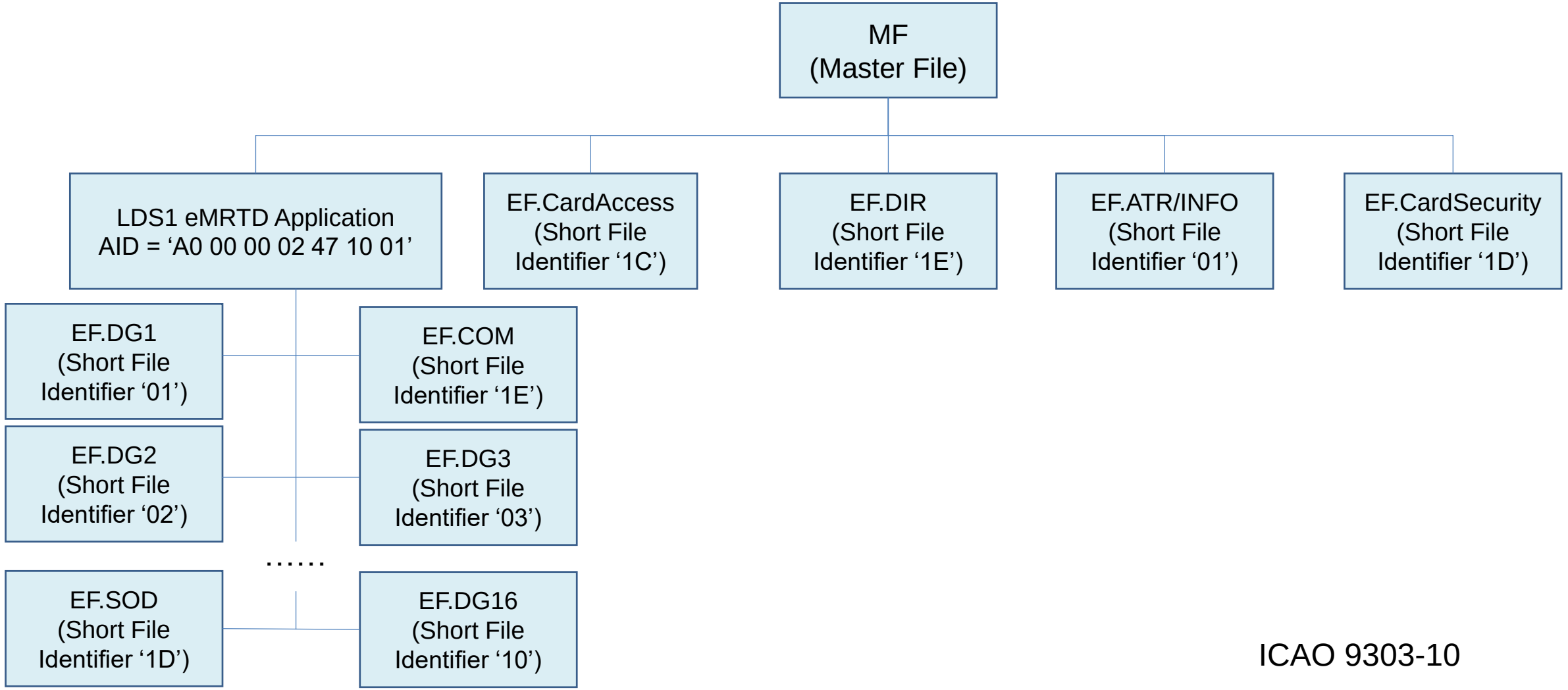
Purpose	Selecting the LDS Application using the AID (robustness tests)
Version	2.04
References	[R1] Part 10
Profile	ICAO, Plain
Preconditions	LDS application MUST NOT be selected.
Test scenario	1. Send the following SelectApplication APDU to the eMRTD. => '00 A4 04 0C 07 A0 00 00 02 47 10 02' 2. Send the following SelectApplication APDU to the eMRTD. => '00 A4 84 0C 07 A0 00 00 02 47 10 01' 3. Send the following SelectApplication APDU to the eMRTD. => '00 A4 04 8C 07 A0 00 00 02 47 10 01' 4. Send the following SelectApplication APDU to the eMRTD. => '00 A4 04 0C 08 A0 00 00 02 47 10 01' 5. Send the following SelectApplication APDU twice to the eMRTD. => '00 A4 04 0C 07 A0 00 00 02 47 10 01' => '00 A4 04 0C 07 A0 00 00 02 47 10 01'
Expected results	1. The APDU has an invalid AID that does not belong to LDS application. Therefore, the eMRTD MUST return an ISO checking error or ISO execution error. 2. The APDU has an invalid P1 parameter. Therefore, the eMRTD chip MUST return an ISO checking error or ISO execution error. 3. The APDU has an invalid P2 parameter. Therefore, the eMRTD chip MUST return an ISO checking error or ISO execution error. 4. The APDU has an invalid LC parameter. Therefore, the eMRTD chip MUST return an ISO checking error or ISO execution error. 5. The application MUST be selected successfully even it was already selected before. Therefore, the eMRTD MUST return the status bytes '90 00' twice.
Postconditions	LDS application is selected.

I Usually Start with Select (00:A4) Command
我通常會從選取 (00:A4) 指令開始



Select MF Root

LDS1 eMRTD Application



ICAO 9303-10

Data Group	EF Name	Short EF Identifier	EF Identifier	Tag
Common	EF.COM	1E	01 1E	60
DG1	EF.DG1	01	01 01	61
DG2	EF.DG2	02	01 02	75
DG3	EF.DG3	03	01 03	63
DG4	EF.DG4	04	01 04	76
DG5	EF.DG5	05	01 05	65
DG6	EF.DG6	06	01 06	66
DG7	EF.DG7	07	01 07	67
DG8	EF.DG8	08	01 08	68
DG9	EF.DG9	09	01 09	69
DG10	EF.DG10	0A	01 0A	6A
DG11	EF.DG11	0B	01 0B	6B
DG12	EF.DG12	0C	01 0C	6C
DG13	EF.DG13	0D	01 0D	6D
DG14	EF.DG14	0E	01 0E	6E
DG15	EF.DG15	0F	01 0F	6F
DG16	EF.DG16	10	01 10	70
Document Security Object	EF.SOD	1D	01 1D	77
Common	EF.CARDACCESS	1C	01 1C	
Common	EF.ATR/INFO	01	2F 01	
Common	EF.CardSecurity	1D	01 1D	

讀取 EF.CardAccess

```
1b 00 20 fa f2 ce 07 ce  ff ff 00 00 00 00 09 00
01 01 00 01 00 01 03 00  00 00 00
```

```
6f0000000b005900000000000700a4020c02011cb2
```

4055	68.073981	host	1.1.1	USB	48	URB_BULK out
4056	68.074061	1.1.1	host	USB	27	URB_BULK out
4057	68.074068	host	1.1.2	USB	27	URB_BULK in
4058	68.087554	1.1.2	host	USB	43	URB_BULK in
4059	68.087785	host	1.1.1	USB		
4060	68.087863	1.1.1	host	USB	27	URB_BULK out
4061	68.087871	host	1.1.2	USB	27	URB_BULK in
4062	68.101778	1.1.2	host	USB		
4063	68.102038	host	1.1.1	USB		
4064	68.102117	1.1.1	host	USB	27	URB_BULK out
4065	68.102123	host	1.1.2	USB	27	URB_BULK in
4066	68.125883	1.1.2	host	USB	149	URB_BULK in

```
6f00000009005a00000000400500b0000006f3
```

```
800000000c005a00000000400831683003d06089000b2
```

```
1b 00 20 fa f2 ce 07 ce  ff ff 00 00 00 00 09 00
00 01 00 01 00 82 03 00  00 00 00
```

```
800000000600590000000000002900092
```

```
1b 00 20 fa f2 ce 07 ce  ff ff 00 00 00 00 09 00
01 01 00 01 00 82 03 7a  00 00 00 80 00 00 00 70
00 5b 00 00 00 00 00 6c  31 68 30 0d 06 08 04 00
7f 00 07 02 02 02 02 01  02 30 0f 06 0a 04 00 7f
00 07 02 02 03 02 02 02  01 02 30 12 06 0a 04 00
7f 00 07 02 02 04 02 04  02 01 02 02 01 12 30 17
06 06 67 81 08 01 01 05  02 01 01 06 0a 04 00 7f
00 07 01 01 04 01 03 30  19 06 09 04 00 7f 00 07
02 02 03 02 30 0c 06 07  04 00 7f 00 07 01 02 02
01 12 90 00 54
```

id-CA-ECDH-AES-CBC-CMAC-128

id-TA

v2

v2

ecdsa-plain-SHA256

- [30 0d [06 08 04 00 7f 00 07 02 02 02] [02 01 02]]
- [30 0f [06 0a 04 00 7f 00 07 02 02 03 02 02] [02 01 02]]
- [30 12 [06 0a 04 00 7f 00 07 02 02 04 02 04] [02 01 02] [02 01 12]]

p521

- [30 17 [06 06 67 81 08 01 01 05] [02 01 01] [06 0a 04 00 7f 00 07 01 01 04 01 03]]
- [30 19 [06 09 04 00 7f 00 07 02 02 03 02] [30 0c [06 07 04 00 7f 00 07 01 02] [02 01 12]]
- 90 00

Active Authentication protocol

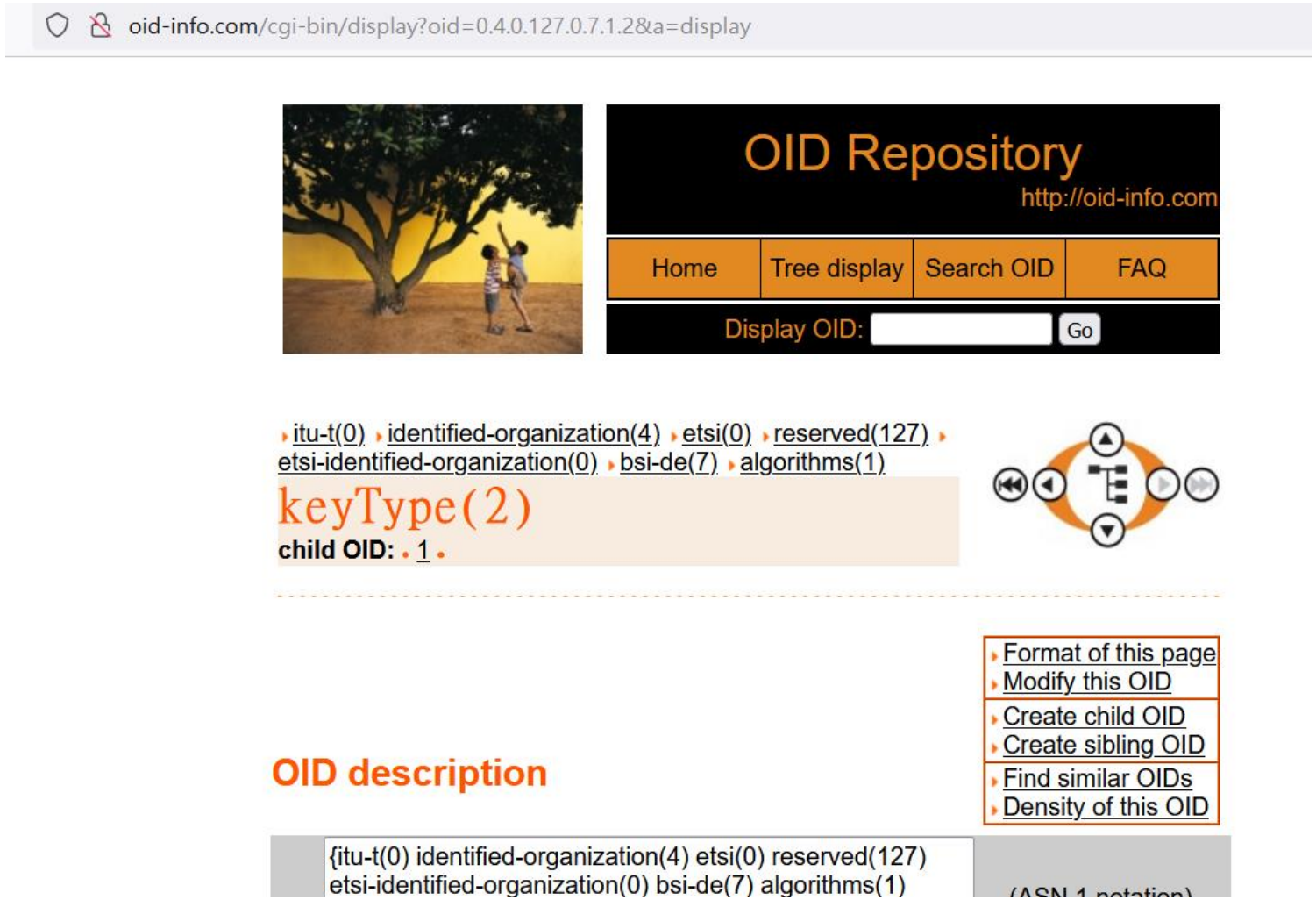
id-CA-ECDH

id-PACE-ECDH-GM-AES-CBC-CMAC-256

bsiEcKeyType

Type	Tag encoding
Boolean	0x01
Integer	0x02
Bitstring	0x03
Octetstring	0x04
Null	0x05
Object identifier	0x06
Sequence	0x30
Sequence of	0x30
Set	0x31
Set of	0x31
UTCTime	0x17

OID Repository



MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

Supplemental Access Control for Machine Readable Travel Documents

Version - 1.01

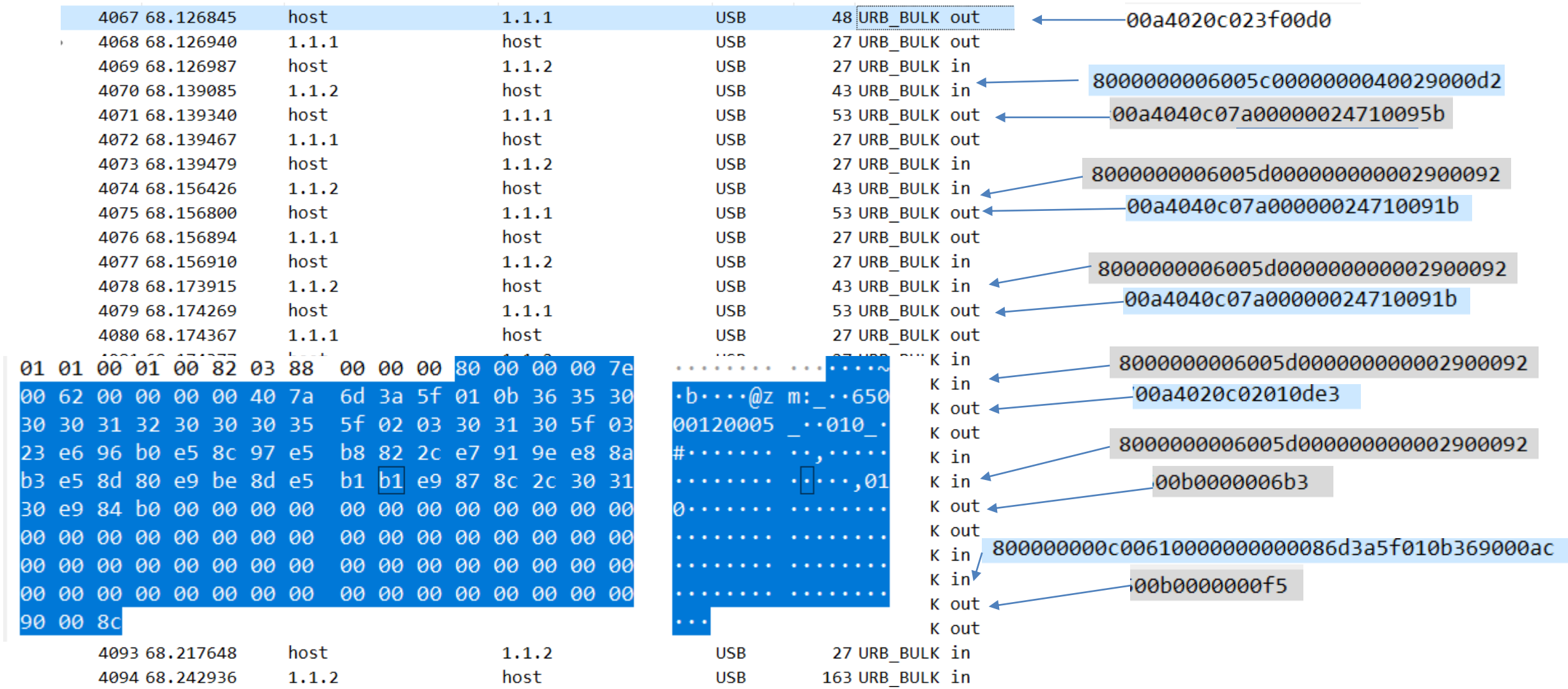
Date – November 11, 2010

Published by authority of the Secretary General

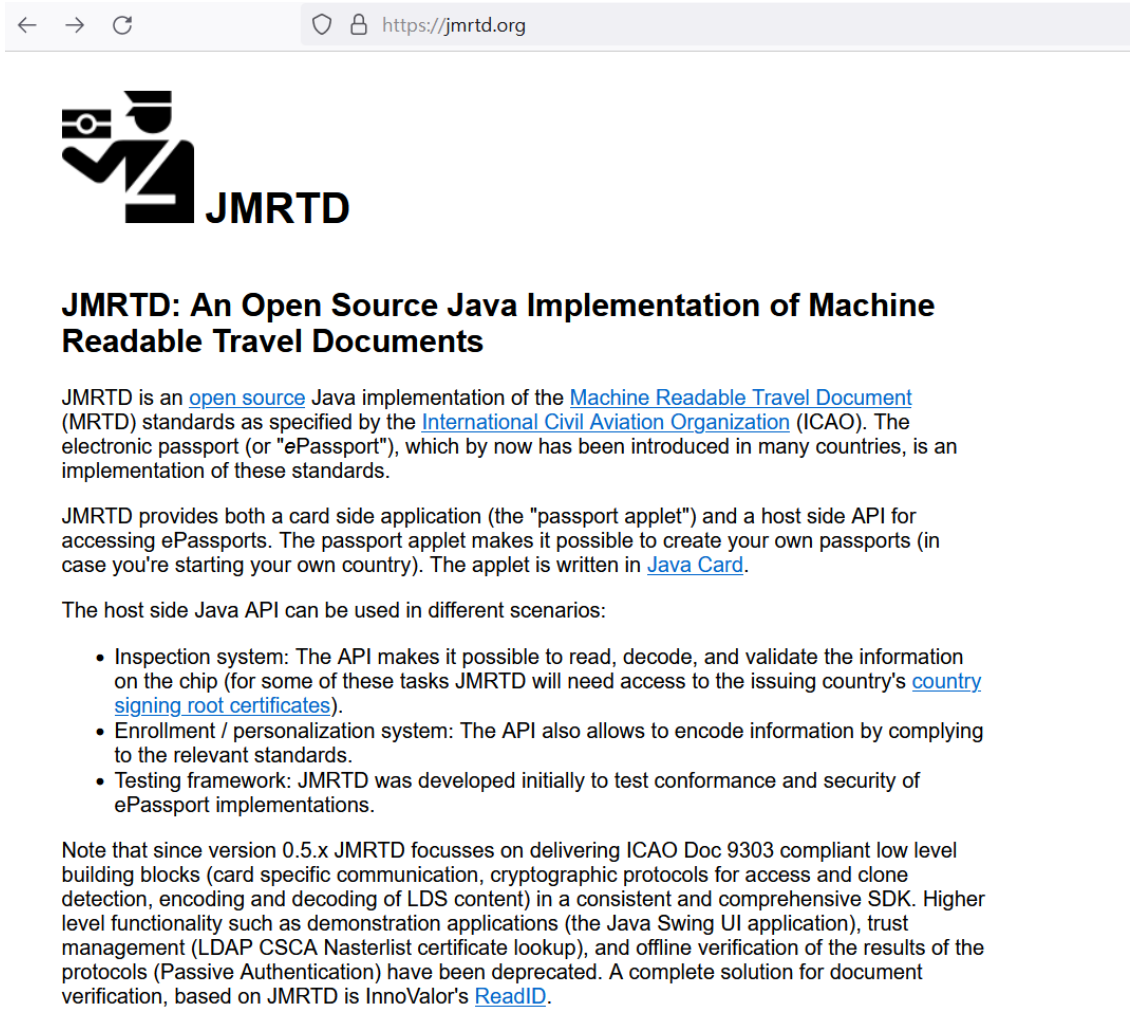
ISO/IEC JTC1 SC17 WG3/TF5
FOR THE
INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: TR-PACE-101-final2.odt
Author	: ISO/IEC JTC1 SC17 WG3/TF5

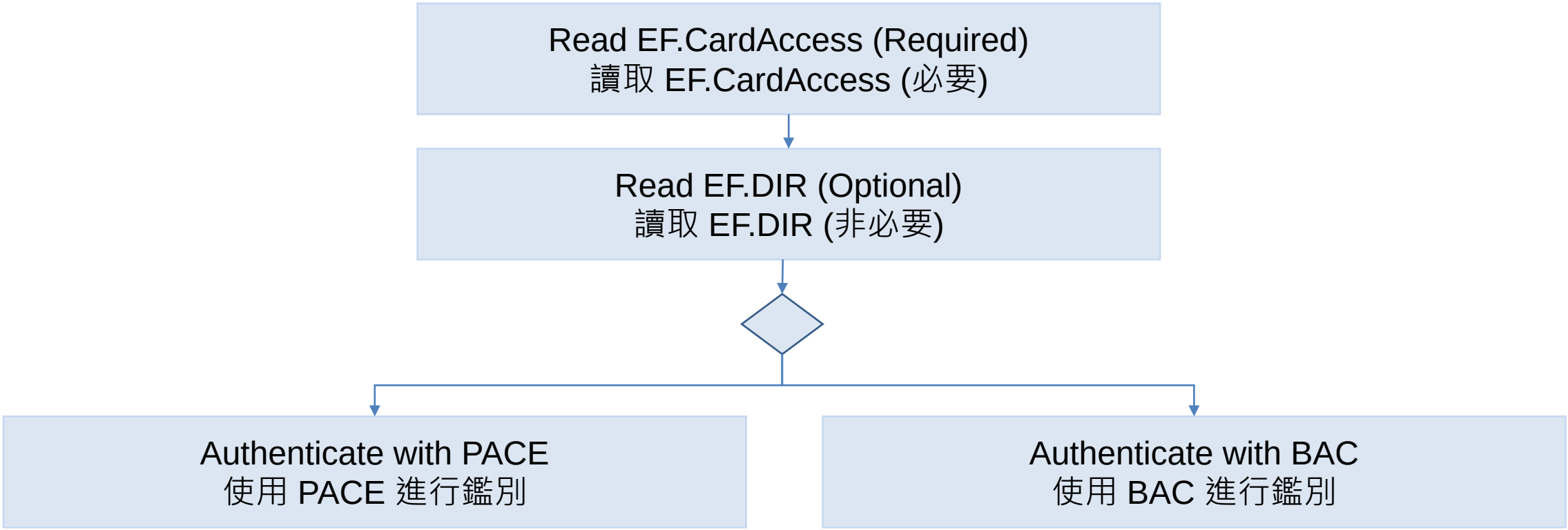
ID	*Name*	*Size*	*Type*	*Reference*
0	1024-bit MODP Group with 160-bit Prime Order Subgroup	1024/160	GFP	[14]
1	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224	GFP	[14]
2	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256	GFP	[14]
3 - 7	RFU			
8	NIST P-192 (secp192r1)	192	ECP	[16], [14]
9	BrainpoolP192r1	192	ECP	[15]
10	NIST P-224 (secp224r1)*	224	ECP	[16], [14]
11	BrainpoolP224r1	224	ECP	[15]
12	NIST P-256 (secp256r1)	256	ECP	[16], [14]
13	BrainpoolP256r1	256	ECP	[15]
14	BrainpoolP320r1	320	ECP	[15]
15	NIST P-384 (secp384r1)	384	ECP	[16], [14]
16	BrainpoolP384r1	384	ECP	[15]
17	BrainpoolP512r1	512	ECP	[15]
18	NIST P-521 (secp521r1)	521	ECP	[16], [14]
19-31	RFU			


4067 68.126845 host 1.1.1 USB 48 URB_BULK out
4068 68.126940 1.1.1 host USB 27 URB_BULK out
4069 68.126987 host 1.1.2 USB 27 URB_BULK in
4070 68.139085 1.1.2 host USB 43 URB_BULK in
4071 68.139340 host 1.1.1 USB 53 URB_BULK out
4072 68.139467 1.1.1 host USB 27 URB_BULK out
4073 68.139479 host 1.1.2 USB 27 URB_BULK in
4074 68.156426 1.1.2 host USB 43 URB_BULK in
4075 68.156800 host 1.1.1 USB 53 URB_BULK out
4076 68.156894 1.1.1 host USB 27 URB_BULK out
4077 68.156910 host 1.1.2 USB 27 URB_BULK in
4078 68.173915 1.1.2 host USB 43 URB_BULK in
4079 68.174269 host 1.1.1 USB 53 URB_BULK out
4080 68.174367 1.1.1 host USB 27 URB_BULK out
01 01 00 01 00 82 03 88 00 00 00 80 00 00 00 7e
00 62 00 00 00 00 40 7a 6d 3a 5f 01 0b 36 35 30
30 30 31 32 30 30 30 35 5f 02 03 30 31 30 5f 03
23 e6 96 b0 e5 8c 97 e5 b8 82 2c e7 91 9e e8 8a
b3 e5 8d 80 e9 be 8d e5 b1 b1 e9 87 8c 2c 30 31
30 e9 84 b0 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
90 00 8c
K in
K out
K out
K in
K out
K out
K in
K in
K out
K out
4093 68.217648 host 1.1.2 USB 27 URB_BULK in
4094 68.242936 1.1.2 host USB 163 URB_BULK in
00a4020c023f00d0
8000000006005c00000000400290000d2
00a4040c07a000000024710095b
8000000006005d000000000002900092
00a4040c07a000000024710091b
8000000006005d000000000002900092
00a4040c07a000000024710091b
8000000006005d000000000002900092
00a4020c02010de3
8000000006005d000000000002900092
00b0000006b3
800000000c006100000000000086d3a5f010b369000ac
00b0000000f5

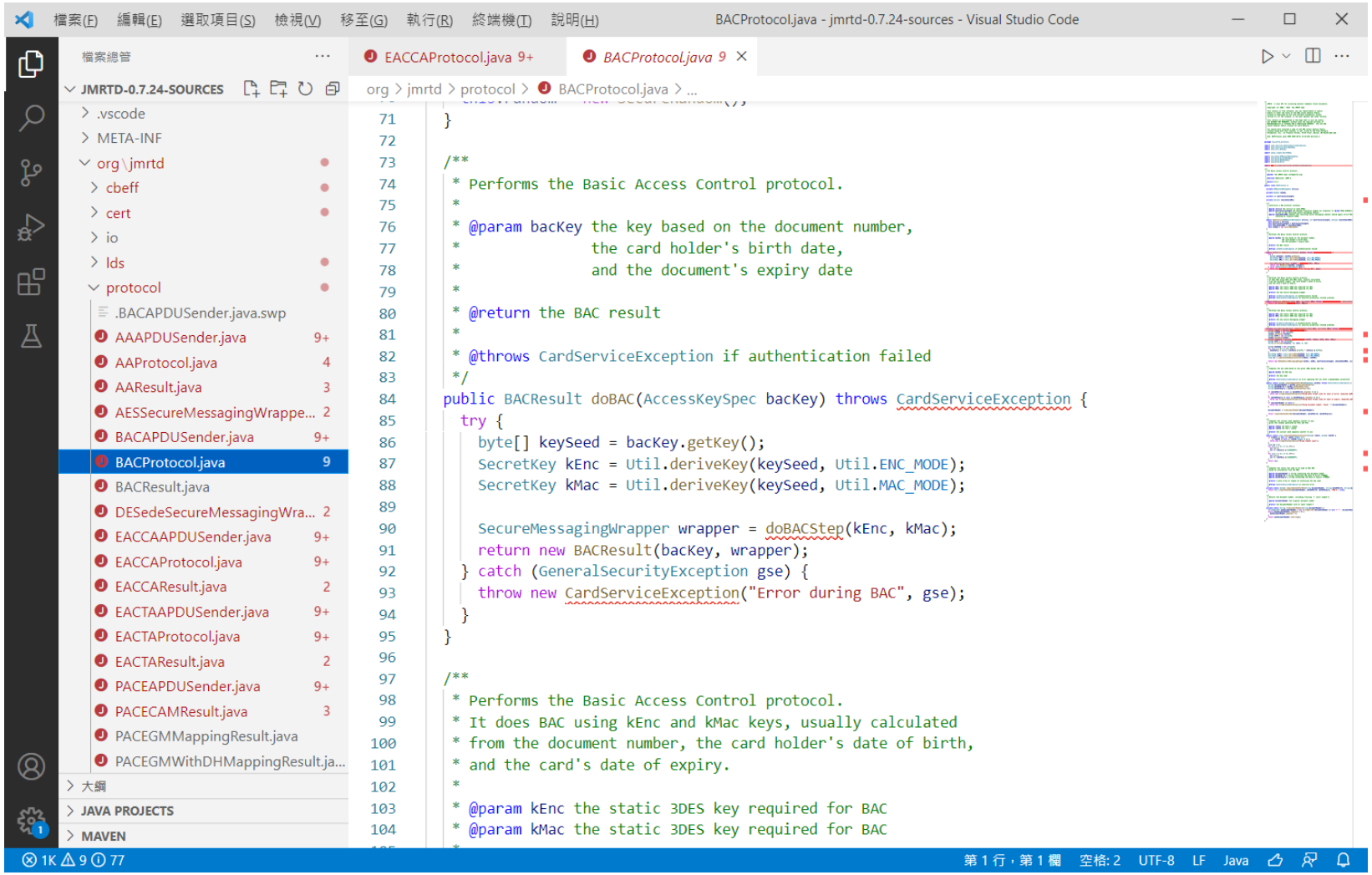
Learning from JMRTD
從 JMRTD 中學習



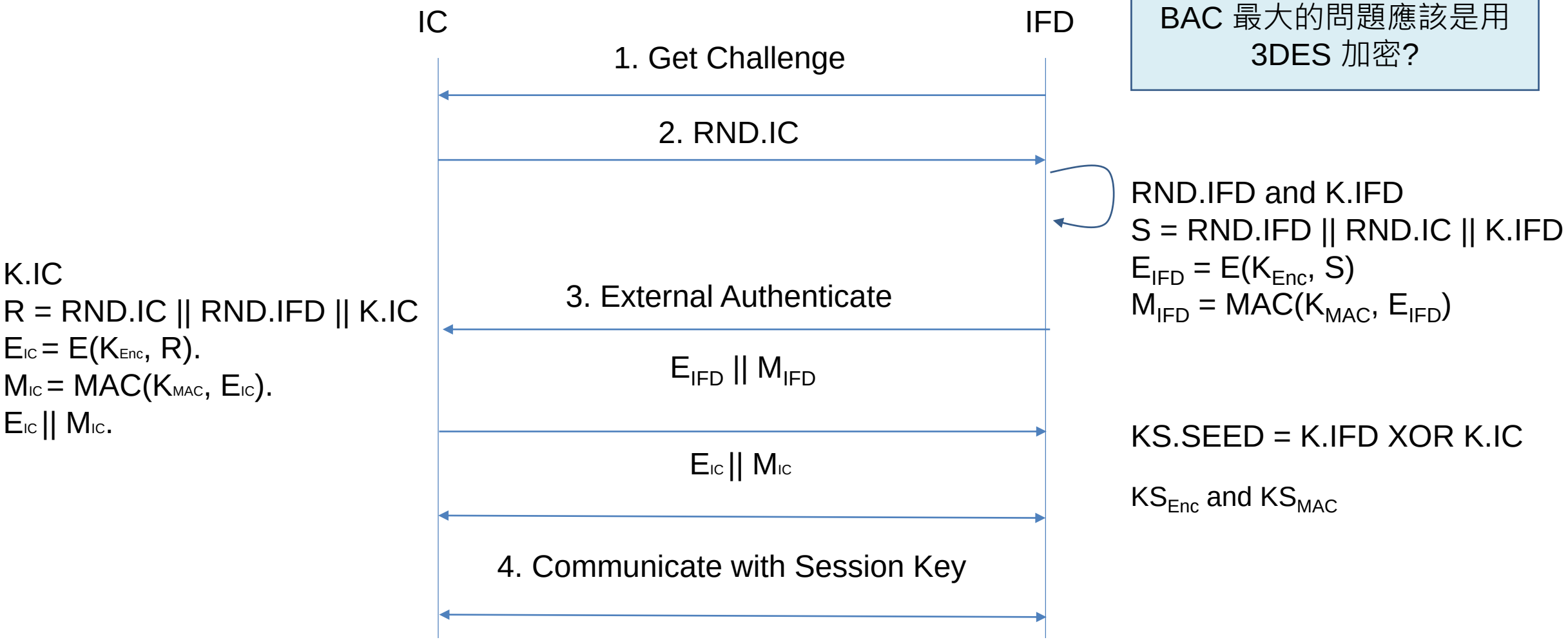
Authentication Process
鑑別程序



Starting 1 January 2018, eMRTD chips implementing PACE only
2018/1/1 後的 eMRTD 晶片只實作 PACE


檔案(F) 編輯(E) 選取項目(S) 檢視(V) 移至(G) 執行(R) 終端機(T) 說明(H)
BACProtocol.java - jmrtd-0.7.24-sources - Visual Studio Code
檔案總管
EACCAProtocol.java 9+
BACProtocol.java 9
org > jmrtd > protocol > BACProtocol.java > ...
JMRTD-0.7.24-SOURCES
.vscode
META-INF
org\jmrtd
cbeff
cert
io
lds
protocol
.BACAPDUSender.java.swp
AAAPDUSender.java 9+
AAProtocol.java 4
AAResult.java 3
AESSecureMessagingWrappe... 2
BACAPDUSender.java 9+
BACProtocol.java 9
BACResult.java
DESedeSecureMessagingWra... 2
EACCAAPDUSender.java 9+
EACCAProtocol.java 9+
EACCAResult.java 2
EACTAAPDUSender.java 9+
EACTAProtocol.java 9+
EACTAResult.java 2
PACEAPDUSender.java 9+
PACECAMResult.java 3
PACEGMMappingResult.java
PACEGMWithDHMappingResult.ja...
大綱
JAVA PROJECTS
MAVEN
71 }
72
73 /**
74 * Performs the Basic Access Control protocol.
75 *
76 * @param bacKey the key based on the document number,
77 * the card holder's birth date,
78 * and the document's expiry date
79 *
80 * @return the BAC result
81 *
82 * @throws CardServiceException if authentication failed
83 */
84 public BACResult doBAC(AccessKeySpec bacKey) throws CardServiceException {
85 try {
86 byte[] keySeed = bacKey.getKey();
87 SecretKey kEnc = Util.deriveKey(keySeed, Util.ENC_MODE);
88 SecretKey kMac = Util.deriveKey(keySeed, Util.MAC_MODE);
89
90 SecureMessagingWrapper wrapper = doBACStep(kEnc, kMac);
91 return new BACResult(bacKey, wrapper);
92 } catch (GeneralSecurityException gse) {
93 throw new CardServiceException("Error during BAC", gse);
94 }
95 }
96
97 /**
98 * Performs the Basic Access Control protocol.
99 * It does BAC using kEnc and kMac keys, usually calculated
100 * from the document number, the card holder's date of birth,
101 * and the card's date of expiry.
102 *
103 * @param kEnc the static 3DES key required for BAC
104 * @param kMac the static 3DES key required for BAC
⊗ 1K ⚠ 9 ⓘ 77
第 1 行，第 1 欄 空格: 2 UTF-8 LF Java

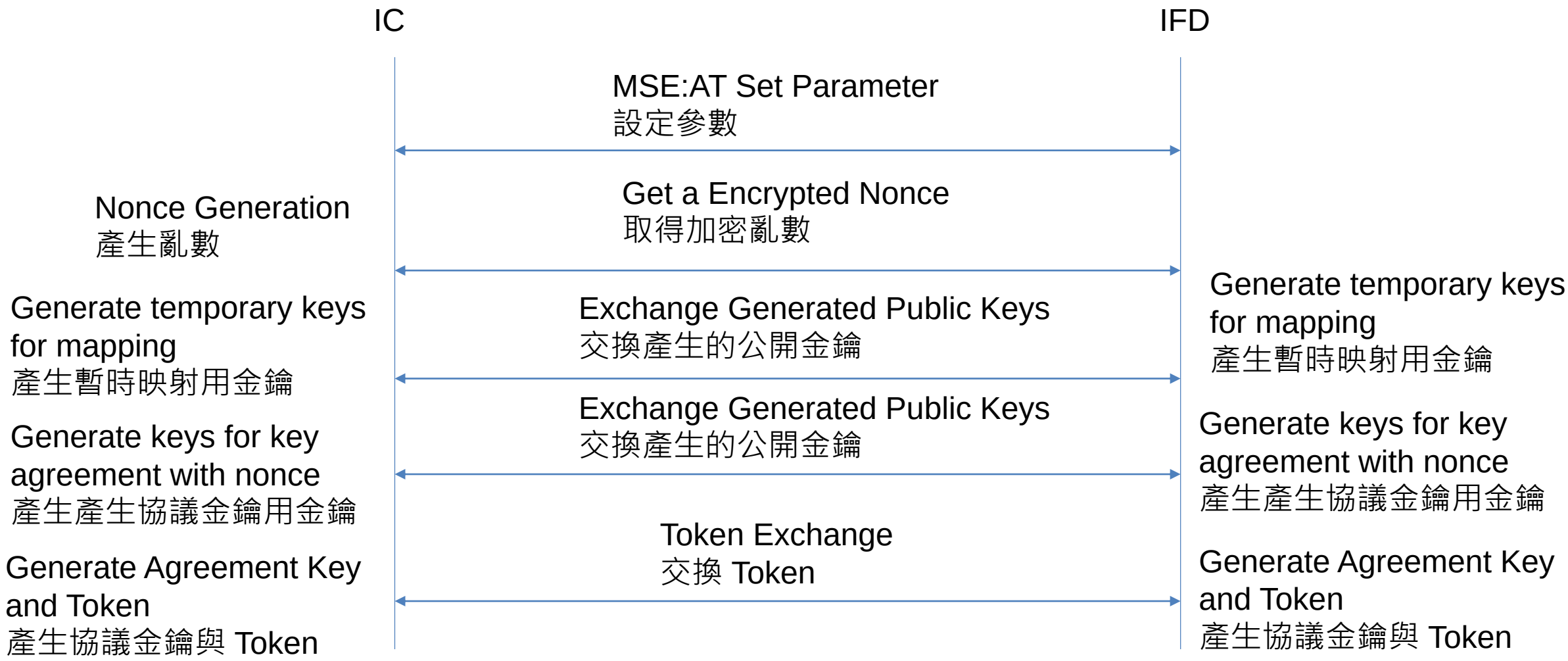
Process of BAC
BAC 的運作程序



The biggest issue of BAC is using 3DES?
BAC 最大的問題應該是用 3DES 加密?

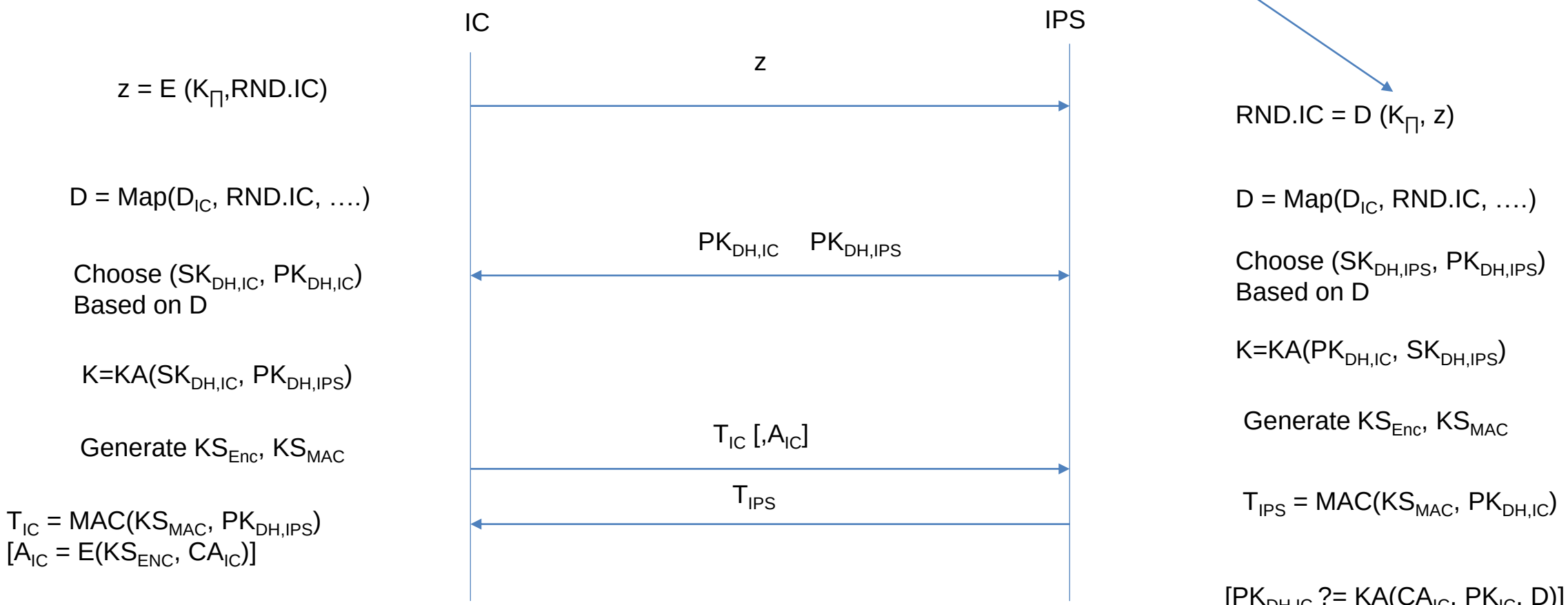
Process of PACE GM
PACE GM 的運作程序

PACEInfo has been obtained
之前已取得 PACE 參數



Password	Encoding
MRZ	SHA-1(DOC Number || DoB || DoE)
CAN	ISO 8859-1 Encoded String

$KDF_{\prod}(f(\prod),3)$



```
C:\Java\jdk1.8.0_301\bin\java.exe ...
Terminals: [PC/SC terminal InfoThink USB Reader 0]
card: PC/SC card in InfoThink USB Reader 0, protocol T=1, state OK
select applet: 9000
select file DG13: 9000
read binary file DG13: 6D3A5F010B3635303030313230303035F02033031305F0323E696B0E58C97E5B8822CE7919EE88AB3E58D80E9BE8DE5B1B1E9878C2C303130E984B0000000000000000000000000000000000000
Send MSE:AT Command
Response MSE:AT Command: 9000
Send General Authenticate Command 1 to Get a Encrypted Nonce
Response General Authenticate Command 1: 7C1280101329BCE702E26B972609A823E5DB43E39000
Nonce: 1329BCE702E26B972609A823E5DB43E3
General Authenticate Command 2 to Exchange Random Generated Public Keys
Response of General Authenticate Command 2 : 7C818882818504011725D101E1A8BD6F572F16A7AEE1BBBF4036E5DE6774F44344A3F6BB9CAF70FF50A1A7113CD421FF7CC9E9B0BBA273A055E8427A0CD22E3AA061
piccMappingEncodedPublicKey: 04011725D101E1A8BD6F572F16A7AEE1BBBF4036E5DE6774F44344A3F6BB9CAF70FF50A1A7113CD421FF7CC9E9B0BBA273A055E8427A0CD22E3AA0618684F8E9DE353801787F197C2920
General Authenticate Command 3 to Exchange Key for Key Agreement
Response of General Authenticate Command 3: 7C818884818504004390E460DA45EC1C69288FDA5F731BF19DD7212A312F9C692F1EC1682249687E7126F4A467062945B03B5B03274B2C4412A41F0193DACC02F21D3
General Authenticate Command 4 to Exchange Token
Response General Authenticate Command 4: 7C0A86088B9FB5841DF0E8569000
Token match!!!
sselect:99026A868E08396ADA743804335A6A86
select DG11:99026A868E08E4352542F1884F0A6A86
verify:87110168F37CCE28365B64A63A0F998DF7E694990290008E082014B42DB4A855349000
decrypted verified:6D9000
readbinary:8781810183DB0A6D19AFA73C2D9824E685ADF4C5914C2F8AFDAEB202AB42157F4BE962092CF2200D1B57DDFA18DD37EFE3AFA14E742102AC84FF651AFFA16887435DBDBEFEA8C493A9B3C440DA097242061435
decrypted DG11:6D3A5F010B3635303030313230303035F02033031305F0323E696B0E58C97E5B8822CE7919EE88AB3E58D80E9BE8DE5B1B1E9878C2C303130E984B0000000000000000000000000000000000000
```

DG11

S230892738

LIU,DUO-TUO

19671121

AT0000005

20301015

- 6B70[5F040BE69FB3F0A98D9CF0A795A6][5F0500][5F060B[4C49552C44554F2D54554F]][5F070A53323330383932373338][5F08083139363731313231][5F090130][5F0A09415430303030303035][5F0B083230333031303135][5F0C083230323031303135][5F0D1031303030393031393532313030323339]00000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000009000

20201015

100090195210023 9

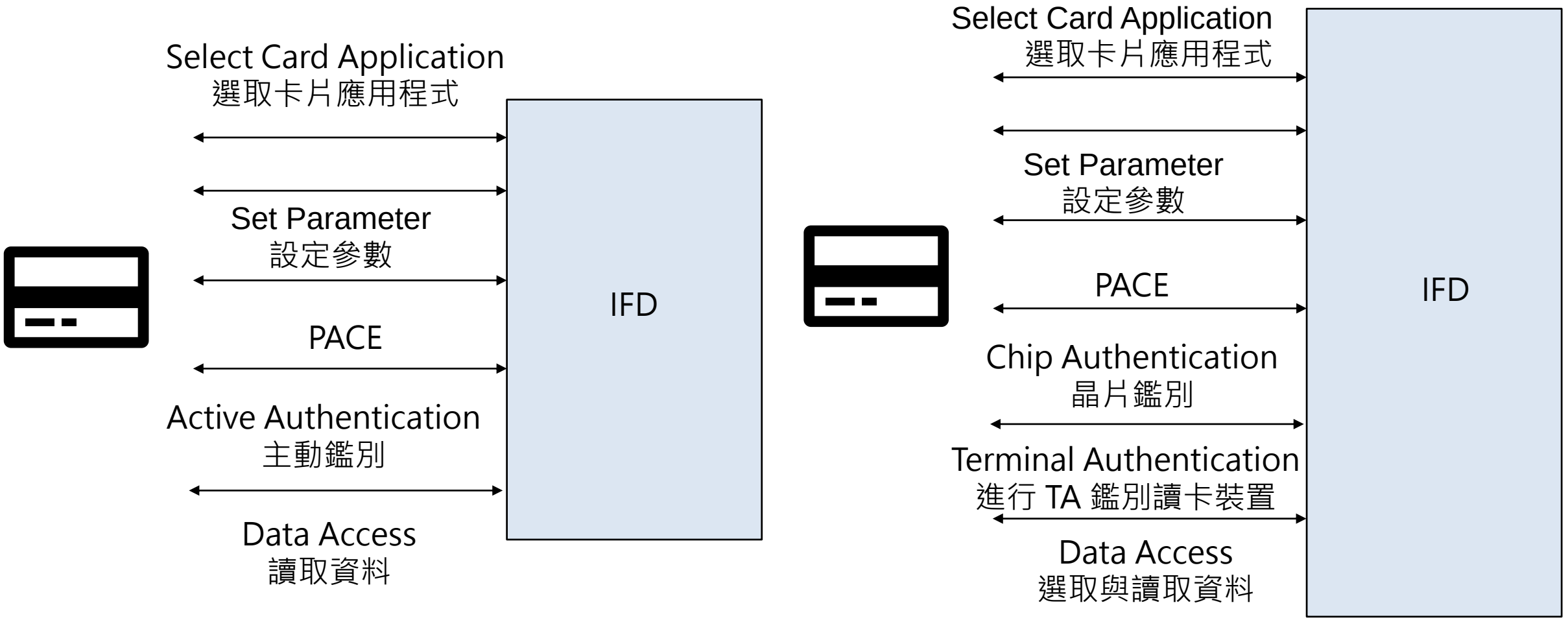
DG12

新北市瑞芳區龍山里010鄰逢甲路２８０號

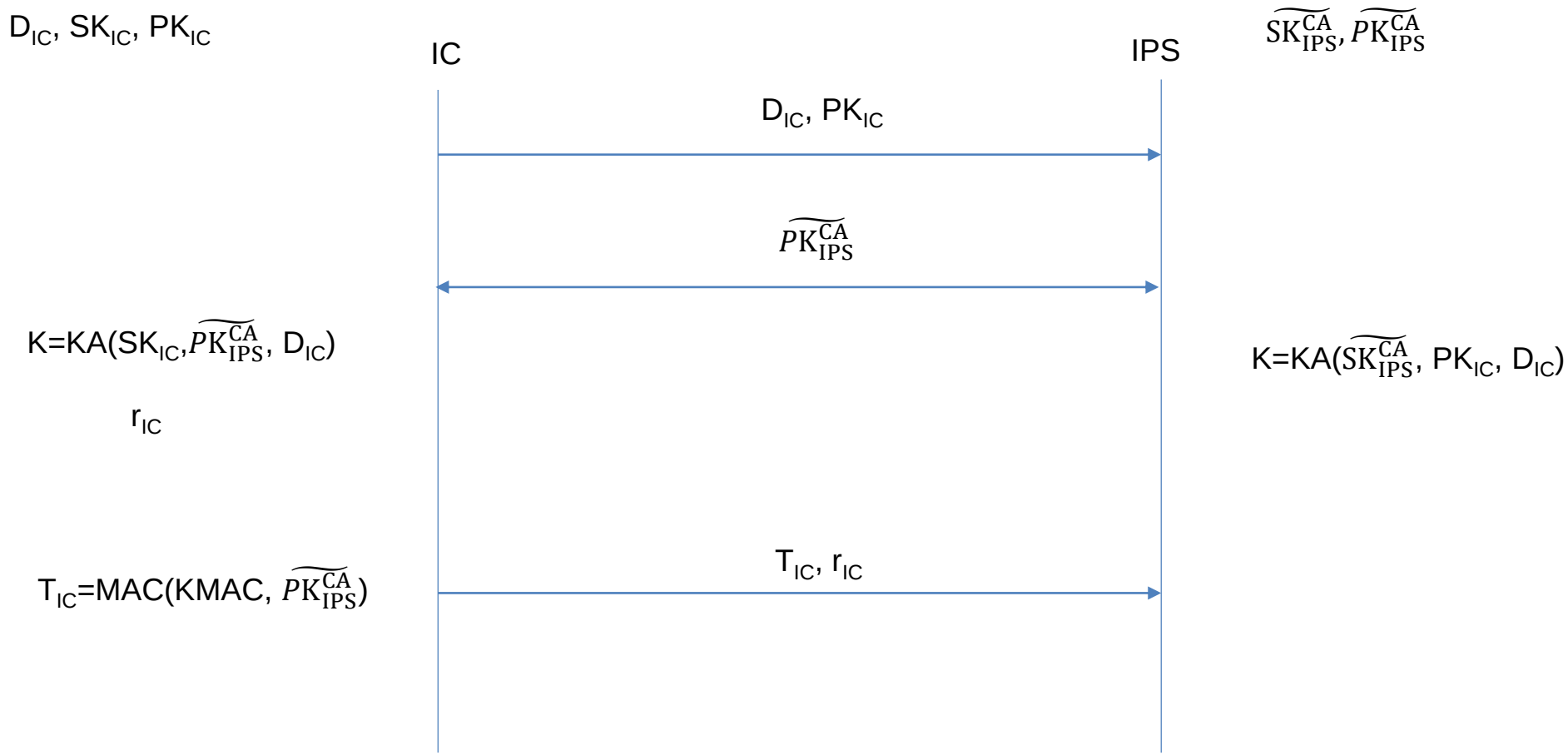
↓

- 6C3D[5F0E0120][5F0F36E696B0E58C97E5B882E7919EE88AB3E58D80E9BE8DE5B1B1E9878C303130E984B0E980A2E794B2E8B7AFEFBC92EFBC98EFBC90E8999F]009000

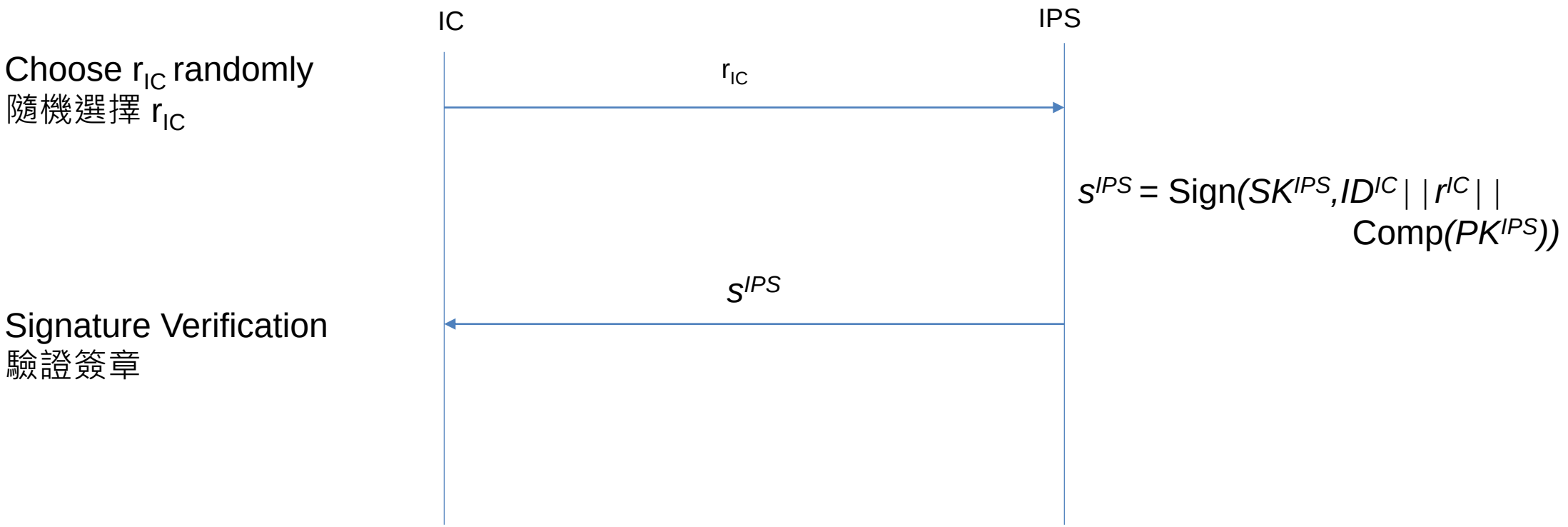
From Accessing Public Data Zone to Encrypted Data Zone
從公開區到加密區

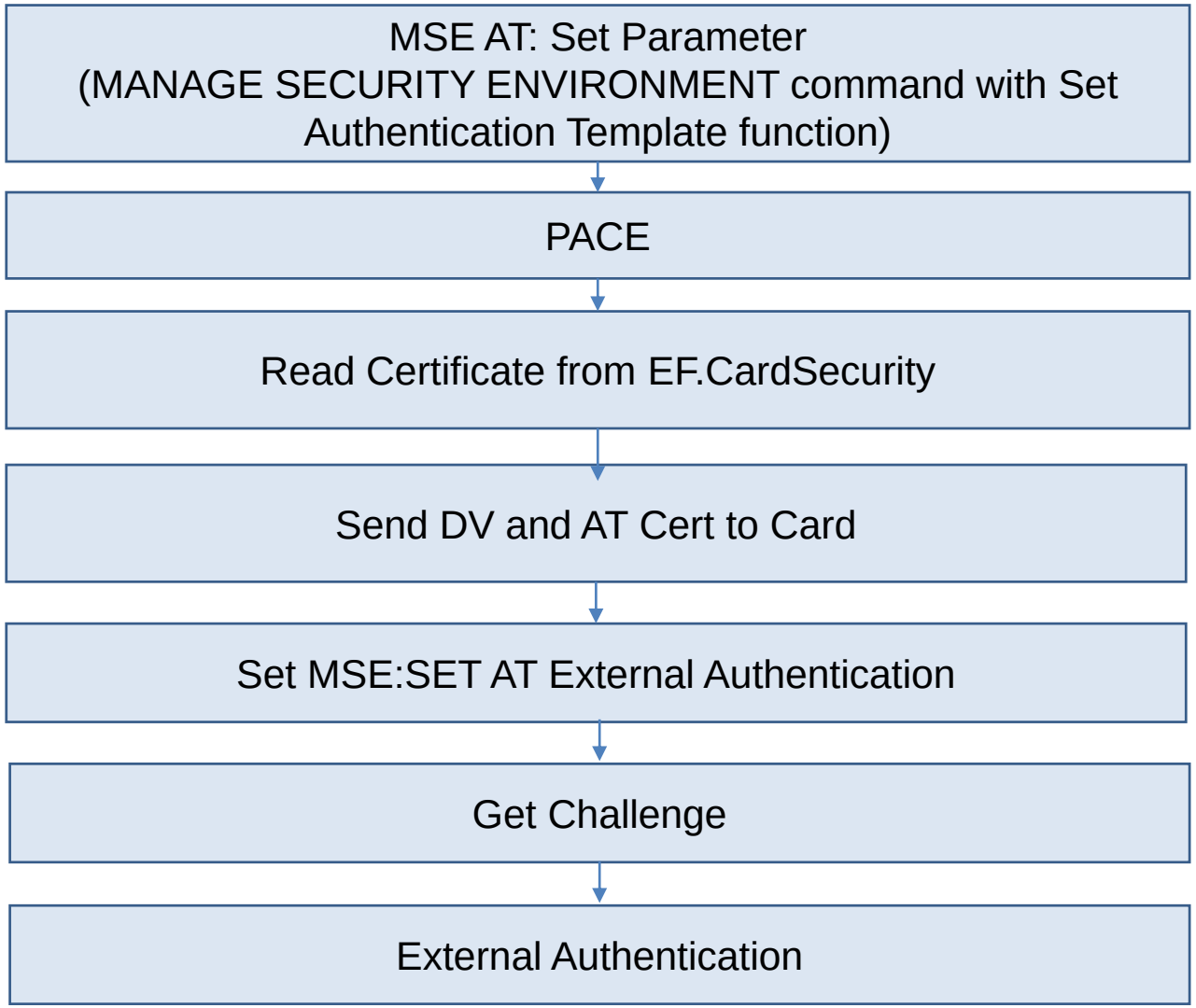


Chip Authentication Process
CA 認證程序



Terminal Authentication Process
TA 認證程序





00 22 c1 a4 27
80 0a 04 00 7f 00 07 02 02 04 02 04
83 01 03
7f 4c 12 06 09 04 00 7f 00 07 03 01 02
02 53 05 00 00 00 60 00
84 01 12

OID || Holder for AT ||
Temporary Public Key

Sign (Temporary IC Public Key in PACE process || challenge || Temporary Public Key)


Certified Host
認可單位
EID Center
EID 中心
DV 憑證與 AT 憑證

[0] Version: 3
SerialNumber: 281567820727501675720798224683179461 89
IssuerDN: C=TW,O=行政院,OU=內政部,OU=戶政司,CN=CSCA
Start Date: Fri Sep 25 11:37:12 CST 2020
Final Date: Tue Mar 25 23:59:59 CST 2031
SubjectDN: C=TW,O=行政院,OU=內政部,OU=戶政司,CN=DS202009250001
Public Key: EC Public Key [c6:7c:fb:e1:c8:4f:e3:4a:4d:23:2a:ab:2e:06:57:77:5e:27:d6:b4]
X: 7db0dd8864840f9856c957715162c28c346c936cc92fdff9c1ffb110c09dac3e7ae067ba4a0b8e93bd86451b860377b85d67da133ee5d10bafaa7068dc88c76056
Y: 96139cc7cfe114c851e96b0d03b851fd16d19b5d61e3cbccf7a135f69e047f7765771600bc6afc633bb17aa8953a7a4ea8cfe22a3b179b8b1b66f8b1340b7d97dd
Signature Algorithm: SHA256withECDSA
Signature: 308188024201cce9925eccee1a00ba46625a6c13c0a70c3dc9bb368253c6917c3f399bc4c20087e0f3f1595ae193ee474cafebc386f8a40aa5040103
2060314d2b400ed66b20ad0242008800e154df65aeb9bae33d7bb45f1fd6800a8e335c2a21eba5ae033c56f06e29384ac5308654ca0fbd98b19e5e29
cdace675d157c66e09a49fa69b5be91d2b3f25
Extensions:
critical(false) 2.5.29.16 value = Sequence
Tagged [0] IMPLICIT
DER Octet String[15]
Tagged [1] IMPLICIT
DER Octet String[15]
critical(false) 2.5.29.35 value = Sequence
Tagged [0] IMPLICIT
DER Octet String[20]
critical(false) 2.5.29.14 value = DER Octet String[20]
critical(true) KeyUsage: 0x80

7f21 CV_CERTIFICATE
  7f4e CERTIFICATE_BODY
    5f29 PROFILE_IDENTIFIER 0
    42 CA_REFERENCE TW/MOICVCAG1/00001
    7f49 PUBLIC_KEY
      6 OID 0.4.0.127.0.7.2.2.2.2.3
      86 PUBLIC_POINT_Y
040048B5D4E6C2B2E91B3D3DCF5C91E4A0C45BFE98086EBEF6440FFB20326BD5BC978CAACE4BCDA82731DDAE3EF880
BFB4F7A6A5BE30798CF36A2833D9B186A4F916E10022B0E68FEB6CD42FD2ADB52FC30E181BD8A73432E1BB3F7928653B
D4CF3D7727904C36C3B2890527472BCF476323D89192AE82973B0081D7B02C939950C08CF37C
    5f20 HOLDER_REFERENCE TW/MOIDVCAG1/00001
    7f4c HOLDER_AUTH_TEMPLATE
      6 OID 0.4.0.127.0.7.3.1.2.2
      53 ROLE_AND_ACCESS_RIGHTS BFFFFFFFFF: DV-domestic/Age Verification, Community ID Verification, Restricted
Identification, Privileged Terminal, CAN Allowed, PIN Management, Install Certificate, Install Qualified Certificate, R-DG1, R-DG2,
R-DG3, R-DG4, R-DG5, R-DG6, R-DG7, R-DG8, R-DG9, R-DG10, R-DG11, R-DG12, R-DG13, R-DG14, R-DG15, R-DG16, R-
DG17, R-DG18, R-DG19, R-DG20, R-DG21, RFU-29, RFU-30, RFU-31, RFU-32, W-DG21, W-DG20, W-DG19, W-DG18, W-DG17
    5f25 EFFECTIVE_DATE 2020-09-17
    5f24 EXPIRATION_DATE 2026-03-17
  5f37 SIGNATURE
A2AD152186C5E700DA2CCAB883B85CAF2AC2892643011452D421E8CE45C311D96A1DA3BFB1992054751B2FDE7AC9DE6F
869400740920519D676C37DF8028A520DBBE96602C317AD338439DBDCBC122338D4990BA6EE30B07E40BDC0F3E2D3F31F
E8D8DAA9C8BF7AC6BA8241F24C4ED94FB2D332016A54FF35F02623AC857C77DAFF6

7f21 CV_CERTIFICATE
  7f4e CERTIFICATE_BODY
    5f29 PROFILE_IDENTIFIER 0
    42 CA_REFERENCE TW/MOIDVCAG1/00001
    7f49 PUBLIC_KEY
      6 OID 0.4.0.127.0.7.2.2.2.2.3
      86 PUBLIC_POINT_Y
0401CF9D14C148602C9A391541614EF330C47C6402E51A41A4A71403434F68F0DFE7D8FF0CEA67700004D41A089
02C8F8D46D583355607FFB673403B44174BCA7BF13B00689BA97774145503F7B1532578BFE80451DA6F13B9C2D2
92B42A0D145559CED9A5DBA7CA01FAAB9EF9F6D634CBD44B3F540E669E0CAC03A9E6B633997C8A2EE3EB
    5f20 HOLDER_REFERENCE TW/MOICA0085/00000
    7f4c HOLDER_AUTH_TEMPLATE
      6 OID 0.4.0.127.0.7.3.1.2.2
      53 ROLE_AND_ACCESS_RIGHTS 0000006000: Authentication-Terminal/R-DG6, R-DG7
    5f25 EFFECTIVE_DATE 2020-11-20
    5f24 EXPIRATION_DATE 2020-11-26
  5f37 SIGNATURE
0151F4D4706828898DC1EA8AE4D9292105D5D7F209FF1DECE8BD5D9645B2049FCC9EF2A5D5F2E5D941CEE8C2E
4BF4E719097CCD48057F4EB79C22F22473C293EC33A0177C1EFE4C1949EDE45DFCCF1E72B4B42F1F1912489269
A6D759F65C2E27EAFF1429C39A76EA7F73DA6739097425C59E742F2893998242300C45435BC276AD8016B

ECC Output ….
ECC 輸出 …..

- 0300A55A05060014A092B6642E095A78929DA3116678EFCB10533BA8A21B7D008A09E287E00B98924BDD55E55C2BF1A50BE5849706A85E27EDB61B857AA65ED3A4A4D0
- 00A55A05060014A092B6642E095A78929DA3116678EFCB10533BA8A21B7D008A09E287E00B98924BDD55E55C2BF1A50BE5849706A85E27EDB61B857AA65ED3A4A4D0

MSE set AT Ext Auth: 9000

Get Challenge: 3864960500415 22C9000

3864960500415 22C

select file DG6: 990290008E08C006DC1E2DB1D3BD9000

decrypted verified:9000

readbinary:878201A101FBE49AE2CA4342F6B0397AE2AAAE9854BF0687740B6D79C12480E2B0DAEA0D051E5733E7EAA544
6EDBD8287EA19D962622E426C12C4DC427BAC21B71DAD16D29ECDD984BF460E6779DB5C29B495C481D036BF6C2CED8
F1B9B25165F04C0DB72F4569D11E757A845D42E5DA88D34BC70F0930696AC657496D88D43261A4C7C502B37B51A0808665
E9B9CB41C05BB579F44168110350A14070EF1879DCBD755678EFB2AB669910CCC1AEEB0A4B0C873B49565CC3762C07D5
7D2CA9289C1F4D8E53206A9899AD5C8BB624FFDAA6B08371606E88CDE55DDFA3293FC3AD2036D56D85105379D288CD78
D7D31C4AA206F2F344A62E9539E2BEFF8B6F3A86FFD3EC86D5281F1DA3D1F4BFA3C3E4C429D762635CB8041840FEFFDE
A3C65AC34C7A209D81A5EFD8C97CC89D9E848593FCB1306D14532F3B41E2141292B00D3535DAF08FF8FE588BC29E2C22
6B1981AB53AA297D7D3F2F09B2A3B8D9C803C4F7F353E89E31F3C10482AB6A661F3680C14C01DF97B58EF9BC275D8DFB
708C518EDF2C8620710ABDE7A1A6A69A33F28EEB71EC533ECD7F52EC7FE8FEABA1261407AB2839D1BD990290008E080A
B6AC20C88203199000

decrypted DG6:66205F1301315F140BE69FB3F0A28A96F0AAA9A85F15005F160830353033393239300000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000009000

1

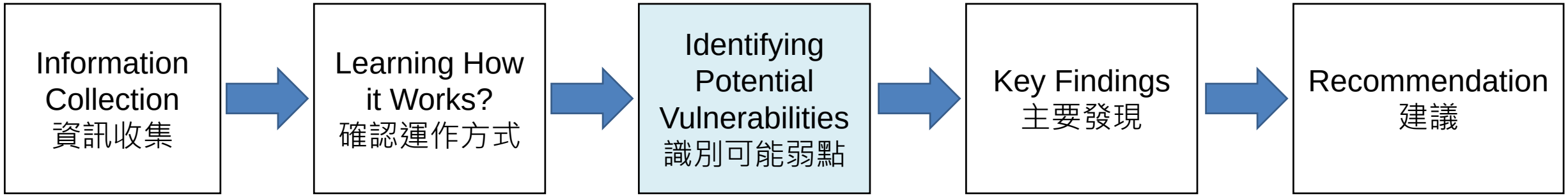
柳糜鼊

05039290 (Random Value)

姜

DG7:67205F1701<u>31</u>5F180B<u>E5A79CF0AFA58EF3BCBB94</u>5F19005F1A08393033393036380009000

Identifying Potential Vulnerabilities
識別可能弱點



Security Mechanism for eMRTD in ICAO 9303-11
eMRTD 晶片的安全機制

Passive Authentication

Active Authentication

Chip Authentication

BAC (Basic Access Control)

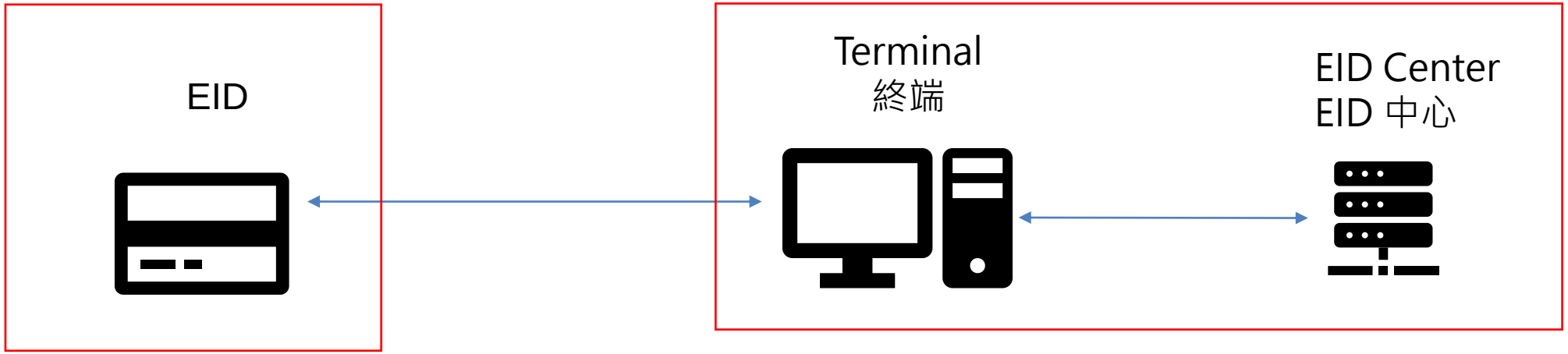
PACE (Password Authenticated Connection Establishment)

Terminal Authentication

Data Encryption

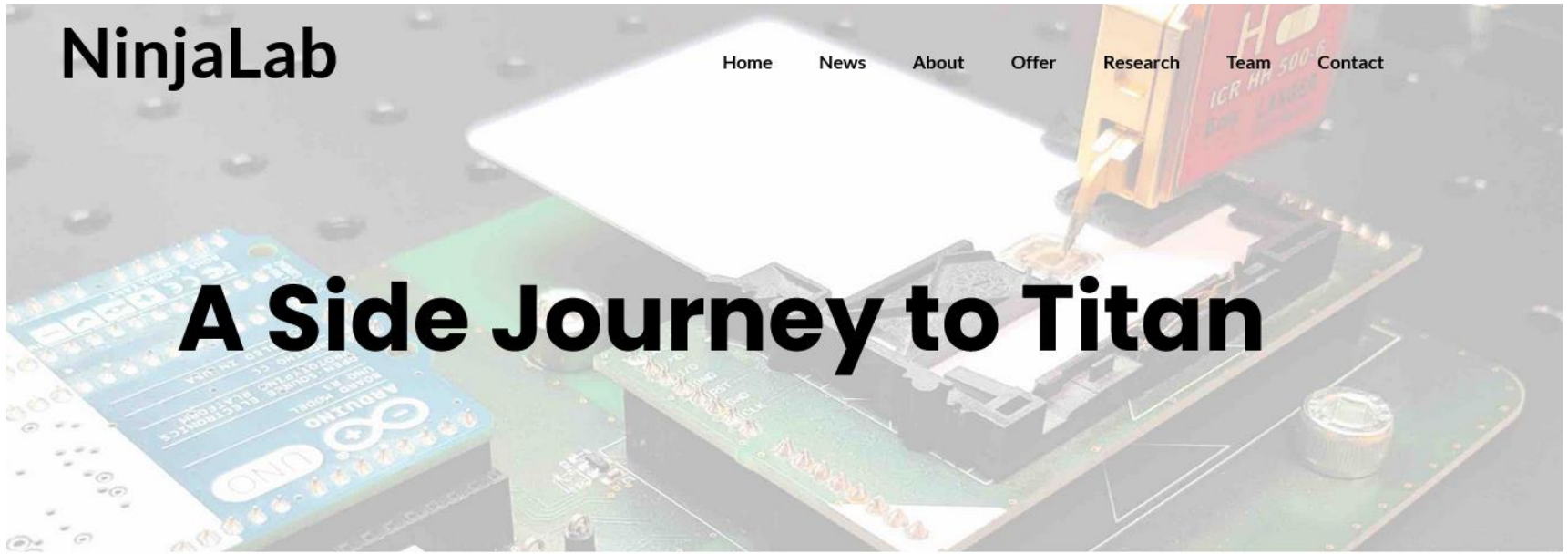
We don't address the chip security issue
本次不考慮晶片安全性

We also don't address security of backend system
本次也不考慮後台安全



Risk Scenario 1: Data can be accessed without permission
風險情境 1：可以在未經鑑別與許可的情況下存取卡片資料

Risk Scenario 2: Cannot use TA to forbid unauthorized
可以在未經鑑別與許可的情況下存取卡片資料



Download the Writeup

https://ninjalab.io/a-side-journey-to-titan/

- Google Titan Security Key (all versions)
- Yubico Yubikey Neo
- Feitian FIDO NFC USB-A / K9
- Feitian MultiPass FIDO / K13
- Feitian ePass FIDO USB-C / K21
- Feitian FIDO NFC USB-C / K40
- NXP J3D081_M59_DF and variants
- NXP J3A081 and variants
- NXP J2E081_M64 and variants
- NXP J3D145_M59 and variants
- NXP J3D081_M59 and variants
- NXP J3E145_M64 and variants
- NXP J3E081_M64_DF and variants

Further Notes

1. The impacted Yubico Yubikey Neo is an old product no more available for sale. All FIDO U2F Yubico Yubikeys currently available on their webstore are based on a newer secure element from Infineon, and are not impacted by our work to our knowledge.

2. The NXP P5 / SmartMX secure microcontroller family and its associated cryptographic library (up to v2.9) impacted by our work is quite old. Since, NXP has released two new generations of secure microcontroller families, the “NXP P60 / SmartMX2” family and now the “NXP P70 / SmartMX3” family. Both are Common Criteria certified (with recent certification process), and are not impacted by our work to our knowledge.

Key Findings
主要發現

Access without TA (only PACE with CAN)
只使用 CAN 進行 PACE 鑑別後的存取

Zone	Accessable
DG1	△ (DG13)
DG2	○
DG3	X (6982)
DG4	X (6982)
DG5	X (6982)
DG6	X (6982)
DG7	X (6982)
DG8	X (6982)

Zone	Accessable
DG9	X (6982)
DG10	△ (DG13)
DG11	○
DG12	○
DG13	○
DG14	△ (DG13)
DG15	○
DG16	△ (DG13)

Access Encrypted Data Zone with Contact and Contactless Interface
使用接觸式與非接觸式介面存取加密區

```
MSE set AT Ext Auth: 9000
Get Challenge: 7B151C3BBF9722639000
7B151C3BBF972263
select file DG6: 990290008E08A3E82067E90437F09000
decrypted verified:9000
readbinary:878201A10153EFBF4AE8A52DEF84ADD975A9651C8558DEE98
decrypted DG6:66205F1301315F140BE69FB3F0A28A96F0AAA9A85F1500
```

Contact Interface
接觸式介面

```
MSE set AT Ext Auth: 9000
Get Challenge: B3CDDBD5CD0B3C6A9000
B3CDDBD5CD0B3C6A
select file DG6: 990290008E0888BEF01687464ABB9000
decrypted verified:9000
readbinary:990269828E087C07153575622A456982
decrypted DG6:6982
```

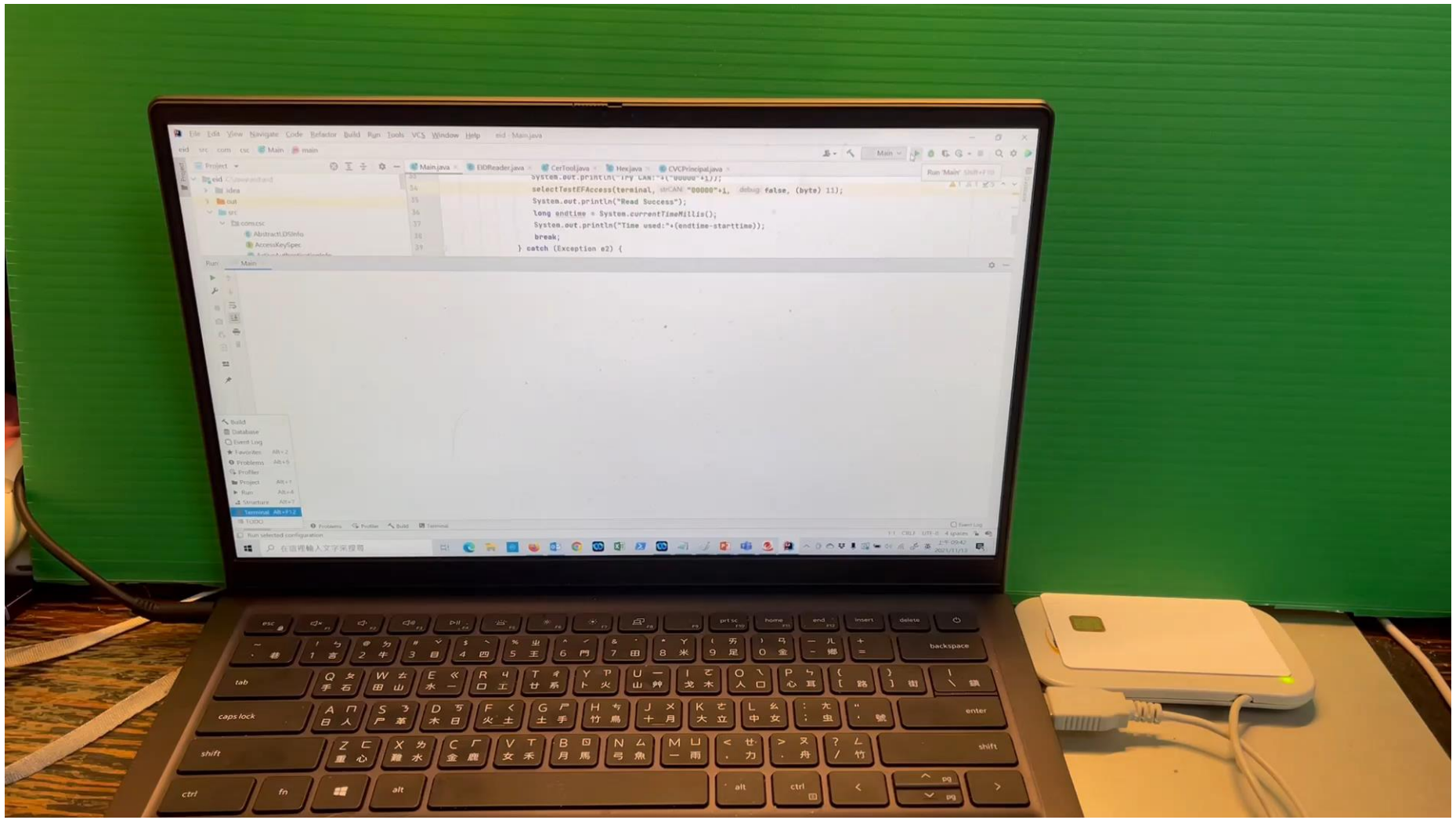
Contactless Interface
非接觸式介面

7F218201747F4E81E85F290100421054574D4F4944564341473130303030317F498194060A04007F0007020202
02038681850401CF9D14C148602C9A391541614EF330C47C6402E51A41A4A71403434F68F0DFE7D8FF0CEA
67700004D41A08902C8F8D46D583355607FFB673403B44174BCA7BF13B00689BA97774145503F7B1532578B
FE80451DA6F13B9C2D292B42A0D145559CED9A5DBA7CA01FAAB9EF9F6D634CBD44B3F540E669E0CAC03
A9E6B633997C8A2EE3EB5F201054574D4F4943413030383530303030307F4C12060904007F00070301020253
0500000060005F25060200010102005F24060200010102065F3781840151F4D4706828898DC1EA8AE4D929210
5D5D7F209FF1DECE8BD5D9645B2049FCC9EF2A5D5F2E5D941CEE8C2E4BF4E719097CCD48057F4EB79C2
2F22473C293EC33A0177C1EFE4C1949EDE45DFCCF1E72B4B42F1F1912489269A6D759F65C2E27EAFF1429
C39A76EA7F73DA6739097425C59E742F2893998242300C45435BC276AD8016B

7F218201747F4E81E85F290100421054574D4F4944564341473130303030317F498194060A04007F0007020202
02038681850401CF9D14C148602C9A391541614EF330C47C6402E51A41A4A71403434F68F0DFE7D8FF0CEA
67700004D41A08902C8F8D46D583355607FFB673403B44174BCA7BF13B00689BA97774145503F7B1532578B
FE80451DA6F13B9C2D292B42A0D145559CED9A5DBA7CA01FAAB9EF9F6D634CBD44B3F540E669E0CAC03
A9E6B633997C8A2EE3EB5F201054574D4F4943413030383530303030307F4C12060904007F00070301020253
0500000060005F25060200010102005F24060200010102075F3781840151F4D4706828898DC1EA8AE4D929210
5D5D7F209FF1DECE8BD5D9645B2049FCC9EF2A5D5F2E5D941CEE8C2E4BF4E719097CCD48057F4EB79C2
2F22473C293EC33A0177C1EFE4C1949EDE45DFCCF1E72B4B42F1F1912489269A6D759F65C2E27EAFF1429
C39A76EA7F73DA6739097425C59E742F2893998242300C45435BC276AD8016B

7f21 CV_CERTIFICATE
  7f4e CERTIFICATE_BODY
    5f29 PROFILE_IDENTIFIER 0
    42 CA_REFERENCE TW/MOIDVCAG1/00001
    7f49 PUBLIC_KEY
      6 OID 0.4.0.127.0.7.2.2.2.2.3
      86 PUBLIC_POINT_Y
0401CF9D14C148602C9A391541614EF330C47C6402E51A41A4A71403434F68F0DFE7D8FF0CEA67700004D41A089
02C8F8D46D583355607FFB673403B44174BCA7BF13B00689BA97774145503F7B1532578BFE80451DA6F13B9C2D2
92B42A0D145559CED9A5DBA7CA01FAAB9EF9F6D634CBD44B3F540E669E0CAC03A9E6B633997C8A2EE3EB
    5f20 HOLDER_REFERENCE TW/MOICA0085/00000
    7f4c HOLDER_AUTH_TEMPLATE
      6 OID 0.4.0.127.0.7.3.1.2.2
      53 ROLE_AND_ACCESS_RIGHTS 0000006000: Authentication-Terminal/R-DG6, R-DG7
    5f25 EFFECTIVE_DATE 2020-11-20
    5f24 EXPIRATION_DATE 2020-11-27
  5f37 SIGNATURE
0151F4D4706828898DC1EA8AE4D9292105D5D7F209FF1DECE8BD5D9645B2049FCC9EF2A5D5F2E5D941CEE8C2E
4BF4E719097CCD48057F4EB79C22F22473C293EC33A0177C1EFE4C1949EDE45DFCCF1E72B4B42F1F1912489269
A6D759F65C2E27EAFF1429C39A76EA7F73DA6739097425C59E742F2893998242300C45435BC276AD8016B

```
      7f4c HOLDER_AUTH_TEMPLATE
         6 OID  0.4.0.127.0.7.3.1.2.2
         53 ROLE_AND_ACCESS_RIGHTS  0000006000: Authentication-Terminal/R
      5f25 EFFECTIVE_DATE  2020-11-20
      5f24 EXPIRATION_DATE  2020-11-27
   5f37 SIGNATURE  0151F4D4706828898DC1EA8AE4D9292105D5D7F209FF1DECE8BD5D
TWMOICVCAG100001
TWMOIDVCAG100001
MSE set cert request: 9000
MSE set cert body: 9000
MSE set cert request: 9000
Error result:00006300
```


selectTestEFAccess(terminal,
System.out.println("Read Success");
long endtime = System.currentTimeMillis();
System.out.println("Time used:"+(endtime-starttime));
break;
} catch (Exception e2) {

```
C:\Java\jdk1.8.0_301\bin\java.exe ...
Terminals: [PC/SC terminal SCR331CL-NTTCom 0]
Try CAN:000000
CAN error
Time used:3941
Try CAN:000001
CAN error
Time used:2407
Try CAN:000002
CAN error
Time used:2397
Try CAN:000003
CAN error
Time used:2404
Try CAN:000004
CAN error
Time used:2403
Try CAN:000005
readbinary:8782026101437BAA23538A04F4C915DEA593250A7D6A32C848CE53A2A8F19C9E20D186D8A8655EE68AFBDF55A754528
decrypted DG11:6B705F040BE69FB3F0A98D9CF0A795A65F05005F060B4C49552C44554F2D54554F5F070A5332333038393237333
Read Success
Time used:2777
```

```
CAN error
Time used:5377
Try CAN:000002
Terminals: [PC/SC terminal SCR331CL-NTTCom 0]
CAN error
Time used:5373
Try CAN:000003
Terminals: [PC/SC terminal SCR331CL-NTTCom 0]
CAN error
Time used:5377
Try CAN:000004
Terminals: [PC/SC terminal SCR331CL-NTTCom 0]
CAN error
Time used:5381
Try CAN:000005
Terminals: [PC/SC terminal SCR331CL-NTTCom 0]
readbinary:87820261015B39E78299E758F95A0943BE54F3D3664D3CBC0EDF059E689EA044332FC27A8F2D8D0E066F03381F078D3FAA34E5CF67581328E25ADA331F0F1899548097005913E285
decrypted DG11:6B705F040BE69FB3F0A98D9CF0A795A65F05005F060B4C49552C44554F2D54554F5F070A5332333038393237333385F0808313936373131323 15F0901305F0A09415430303030
Read Success
Time used:5980
```

The performance of contactless card reading determines the position of card

非接觸式的卡片讀取速度和卡片讀取的穩定性有關

```
Try CAN:000000
CAN error
Time used:2212
Try CAN:000001
CAN error
Time used:581
Try CAN:000002
CAN error
Time used:575
Try CAN:000003
CAN error
Time used:571
Try CAN:000004
CAN error
Time used:579
Try CAN:000005
readbinary:878202610174115592EA958E2F95F8152344345E97C5C09BAB71F2AA23C61D5B6DE2A9CC01B58078F7A7650C5B270B60767B1088B8DABC8E
decrypted DG11:6B705F040BE69FB3F0A98D9CF0A795A65F05005F060B4C49552C44554F2D54554F5F070A5332333038393237333385F0808313936373
Read Success
Time used:891
```

The performance via contact interface is better than performance via contactless interface
接觸式比非接觸式效能要好

63CX: Verify fail, X tries left

驗證失敗，還有 X 次可以嘗試

Ex.

63C3: Verify fail, 3 tries left.

驗證失敗，剩三次可以嘗試

```
Type 4:[illegible]
General Authenticate Command 4 to Exchange Token
Response General Authenticate Command 4: 63C3

Type 4:[illegible]
General Authenticate Command 4 to Exchange Token
Response General Authenticate Command 4: 63C2
```

Summary of Findings
發現摘要

- The data in the Public Data Zone can be accessed via brute force attack against CAN. Therefore, malicious people can access data in a card without contacting a card at most 27 days (2,400,000/86,400~27)

  在可以無線存取的情況下，可以透過 CAN 暴力破解，在不接觸卡片的情況下，取得公開區的資料。如果以讀取一次 2.4 秒計算，2400000/86400~27 天

  - MRZ could be better than CAN

    無線存取可以限制使用 MRZ，增加破解時間

- Cannot inactivate a terminal actively

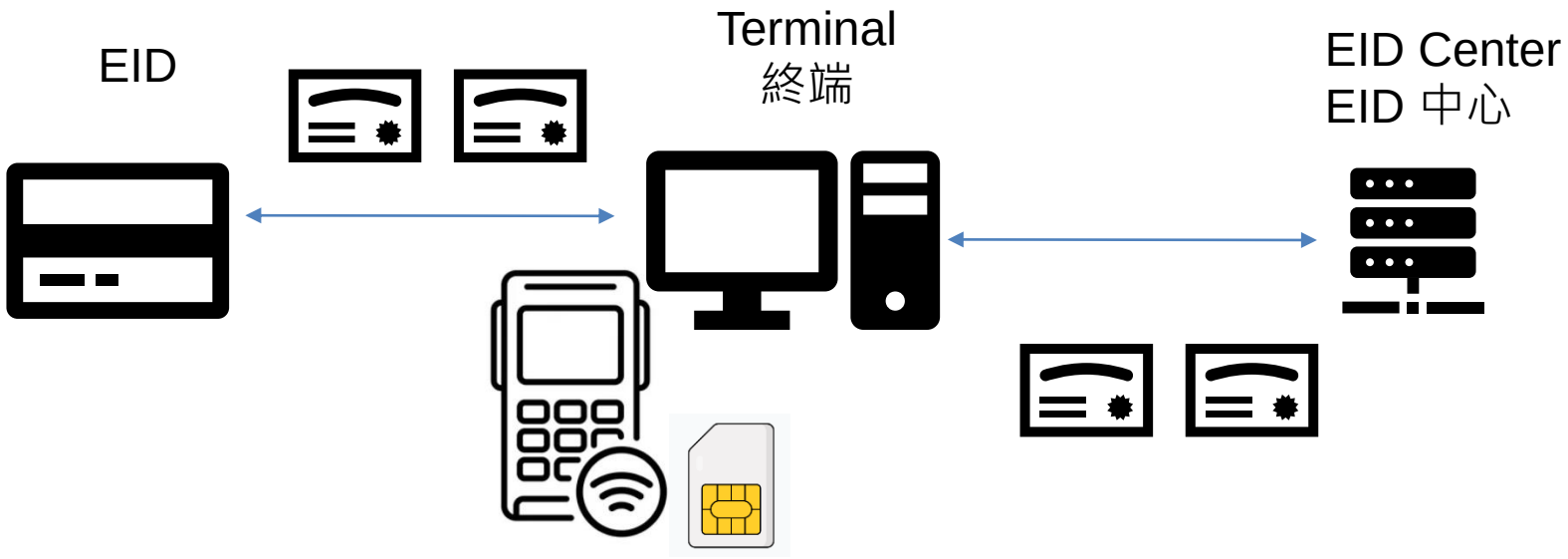
  目前使用 TA 的設計無法主動停用一台讀取終端 (卡片無法主動去讀取 CRL 或呼叫 OCSP)

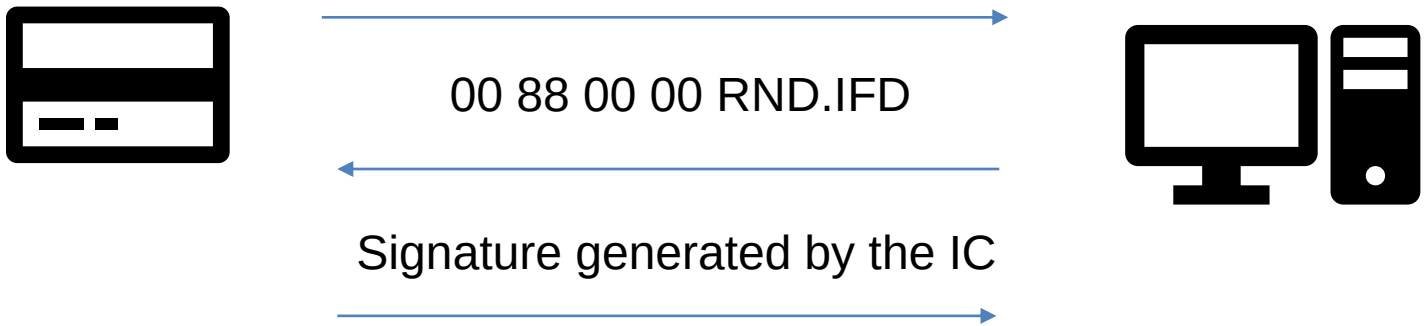
  - Could use SAM to protect terminal private key and shorten the validation time of AT certificate

    如果真要綁定終端，可以採用 SAM 卡保護資料，同時縮短憑證有效期間

- AA mechanism could be misused

  AA 認證機制可能被誤用


EID
Terminal
終端
EID Center
EID 中心


Obtain AA Certificate (DG15)
00 88 00 00 RND.IFD
Signature generated by the IC

Recommendation
建議

Conclusion and Recommendation
結論與建議

- Integrated circuit identification card can improve the security and convenience of using online services. As every national online services may rely on the card, we should consider the security and privacy issues carefully 數位身分識別證可以提升使用數位服務的安全性。而因為國家的身分鑑別服務多半會支援這張卡片，所以其安全與隱私的議題需要特別考量。
- The suspended EID card adopts the specification of ICAO 9303. We did not find critical security issues currently. 目前暫停的 EID 套用 ICAO 9303 的標準。實作上並未發現重大安全議題。
  - The data in the Public Data Zone can be accessed via brute force attack against CAN 可以透過非接觸式介面暴力破解 CAN 讀取卡片資料
- Contactless interface is very important for smart phones. We suggest to keep the interface and adjust the associated function 非接觸式介面在智慧型手機的應用上非常重要，建議能夠保留與善用此介面，並對可存取資料做出調整。
  - 可以考慮支援 FIDO CTAP2
- As the data in the Encrypted Data Zone are not very sensitive, current software-based terminal authentication scheme does not have significant risks. However, terminal binding would bring inconvenience for some applications. 目前加密區當中沒存什麼資料，因此目前採用軟體憑證方式進行終端綁定風險不明顯。反而讀取加密區要綁終端，對於某些應用來說可能會造成不便。

Thank You
感謝各位的聆聽