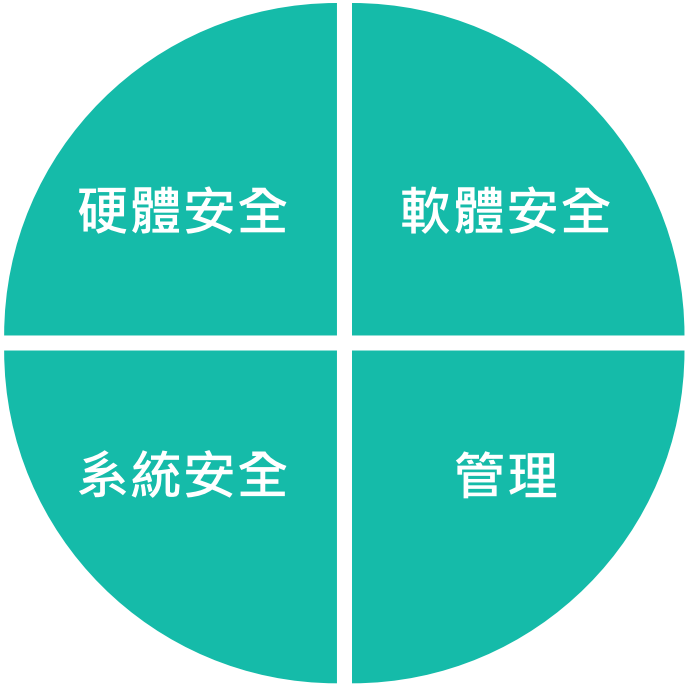
國民身分證晶片化後的資安威脅與個資隱憂

李育杰
中央研究院 資訊科技創新研究中心
TWISC@AS

July 29, 2020

資訊安全所涉及層面甚廣

- 安全晶片
- 讀取設備



- APPs
- API

- 網路
- 伺服器
- Web service

- Insiders Threat
- 內部竊取
  - RSA 2020: Human Element

晶片潛在資安風險

製程風險	可能造成私密金鑰外洩
非接觸式通訊介面	可能造成卡號和無讀取碼保護的資料外洩
自然人憑證功能	晶片卡遺失可能造成電子身份偽裝

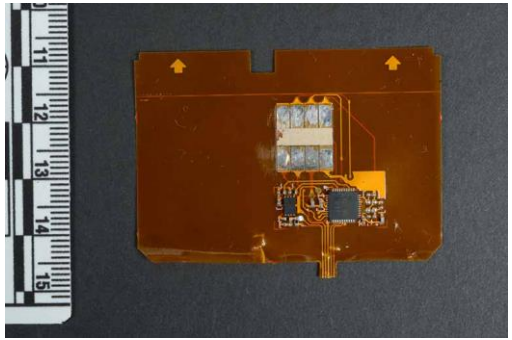
讀卡設備潛在資安風險

讀卡設備本身

可能遭裝設惡意側錄元件(如：Card shimmer，如右下圖)，而資料外洩

連接之運算裝置

可能被植入惡意程式或木馬，而造成資料外洩或中間人攻擊



讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

沒有對讀卡設備做資安規範

根據內政部戶政司New eID簡易問答集，目前 New eID 受三個專法規範：

- 資訊安全：資通安全管理法
- 個資保護：個人資料保護法
- 自然人憑證：電子簽章法

資安弱點

資安威脅

讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

資安弱點

讀卡機可能被加裝側錄元件

- 在出廠時：讀卡機設備商或其員工
- 在讀卡機沒有被安全保護時：駭客

資安威脅

讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

資安弱點

資安威脅

讀卡機所讀的用戶資訊皆會被竊取

讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

沒有對讀卡設備和其連接狀置做資安規範

資安弱點

資安威脅

讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

資安弱點

讀卡機和其連接裝置可能因社交工程攻擊或其它軟體和作業系統之資安弱點，而遭植入惡意程式或木馬

資安威脅

讀卡設備潛在資安風險

讀卡設備本身

連接之運算裝置

目前機制

資安弱點

資安威脅

讀卡機所讀的用戶資訊皆會被竊取

讀卡機連接網際網路，且無建置惡意軟體監控機制，使得被竊取之資訊可輕易地被送出讀卡機

用戶隱私潛在資安風險

用戶資訊自主	用戶無法做到資訊自主，無法控制或掌握特定機關對於自己資訊的取得
用戶數位足跡	內政部擁有用戶數位足跡，可能侵害用戶隱私

用戶隱私潛在資安風險

用戶資訊自主

用戶數位足跡

目前機制

根據內政部戶政司 New eID 簡報，需用機關 (公務、金融及醫院) 可讀取之用戶資訊，由內政部審視其需求，進行控管可讀取之特定欄位

資安弱點

資安威脅

用戶隱私潛在資安風險

用戶資訊自主

用戶數位足跡

目前機制

資安弱點

當用戶提供 eID 卡給需用機關時，無法控制或掌握該機關可以讀取什麼資訊，而且內政部授權該需用機關前，也未取得用戶同意

資安威脅

用戶隱私潛在資安風險

用戶資訊自主

用戶數位足跡

目前機制

資安弱點

資安威脅

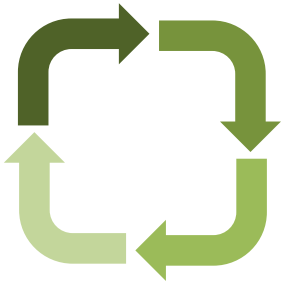
當內政部審視需求不確實，濫發授權憑證時，將可能洩漏過多的用戶資訊給特定機關，而且用戶又無從察覺和判斷

資訊安全無法保證

攻擊技術發展先於防禦技術的發展

攻擊技術進步

防禦技術失效



攻擊技術失效

防禦技術進步

現有防禦技術
無法永久保證有效

資安風險可以管控

- 資安防禦技術在偵測、阻絕、延後系統被攻破的時間。系統被攻破後的風險控管與復原。
- 具有資安概念的國家政策理當追求最小化資安風險，並僅在政策所生之公共利益大於其資安風險時，方為合理可行之國家政策
- 簡言之，**利 > 弊**，且風險可管控，系統能復原!

自然人憑證、悠遊卡均通過安全認證

自然人憑證

Crypto IC 卡片	
實體特性	• 外型尺寸、卡片工作環境溫、濕度標準應符合ISO 7810及7816相關規定。 • EEPROM記憶體至少達32K位元組（含）以上，晶片讀寫次數至少10萬次（含）以上。 • 資料儲存保存時間應至少5年（含）以上。 • 提供多樣化印刷美術設計技術並配合需要使用透明及不透明卡材，增加卡片美觀效果。 • 提供多種材質選擇至少需有PVC。
實體特性	• 正常使用下，卡片印刷部份覆被材質及晶片不可有剝落現象。需出具相關佐證資料或實例說明。 • 卡片長邊、短邊彎曲(bending)、扭曲(torsion)承受限度需優於ISO7816-1檢測水準並出具相關佐證資料。
IC卡之指令、介面規格及功能	• 卡片上各接點之電氣訊號特性、金屬接點尺寸接點位置、卡片通信介面接觸式部分及卡片回應重置訊號（Answer To Reset）需依照ISO 7816相關規定。 • 基本指令：提供符合ISO 7816-4指令集、RSA/DSA 金鑰之產製、匯入、加驗簽章、加解密等指令。 • IC卡介面應符合PKCS#11，CSP規範，需提供IC卡介面應用程式，至少應包括PKCS #11及MS CAPI。出具IC卡片安全規格可資公信佐證資料。 • 可自行產生金鑰對，金鑰產生長度需達RSA 1024 bit（提供憑證管理中心使用則需達 RSA 2048 bit）（含）以上或其他相同安全規格。金鑰不允許被讀出。 • 具備簽章及加解密運算、更改PIN、Secure Mail、 SSL Client Authenticatin等功能並提供應用介面函式庫。 • 高運算效率，如果以 1024 bit內部晶片簽章（RSA_Sign指令），則每次必須小於1秒。 • 必須至少相容於PC/SC介面之讀卡機並詳列所有可使用讀卡機之廠牌、型號、適用作業系統、製造商資料、新台幣計算之定價、台灣地區出售/售後服務經銷商及可購買地點等詳細資訊。自第一期後各期營運承包廠商所提供之IC卡需提出相容於第一期計畫起所使用之讀卡機之解決方案。

資料來源 – https://moica.nat.gov.tw/wisdom.html

悠遊卡

	MIFARE Classic MIFARE Classic EV1
射頻介面	ISO/IEC 14443-2，TYPE A
通訊協定	ISO/IEC 14443-3
UID碼	UID：7位元組，RID：4位元組（無UID）
通訊速度	106Kbps
資料儲存容量	144bytes
驗證金鑰種類	Crypot-1
機卡驗證類型	三重認證
機卡通訊加密類型	Encrypted
共同準則認證類型	無

資料來源 – https://zh.wikipedia.org/wiki/MIFARE

通過多項安全認證不表示絕對安全

- 自然人憑證 – 2013 年鄭振牟教授曾破解過憑證金鑰系統。https://www.ithome.com.tw/node/82731
- 悠遊卡 – 2010 年鄭振牟教授在駭客年會上，演示以監聽封包方式，竄改悠遊卡餘額。https://www.ithome.com.tw/node/63075
- 悠遊卡 – 2011 年號稱「絕對不可能被破解」的儲值加密系統遭駭客破解，並在市面上消費。https://news.ltn.com.tw/news/focus/paper/527166

為何悠遊卡仍繼續被使用？

1. 被盜用時，容易偵測
2. 成本考量
3. 有罰則與法律責任

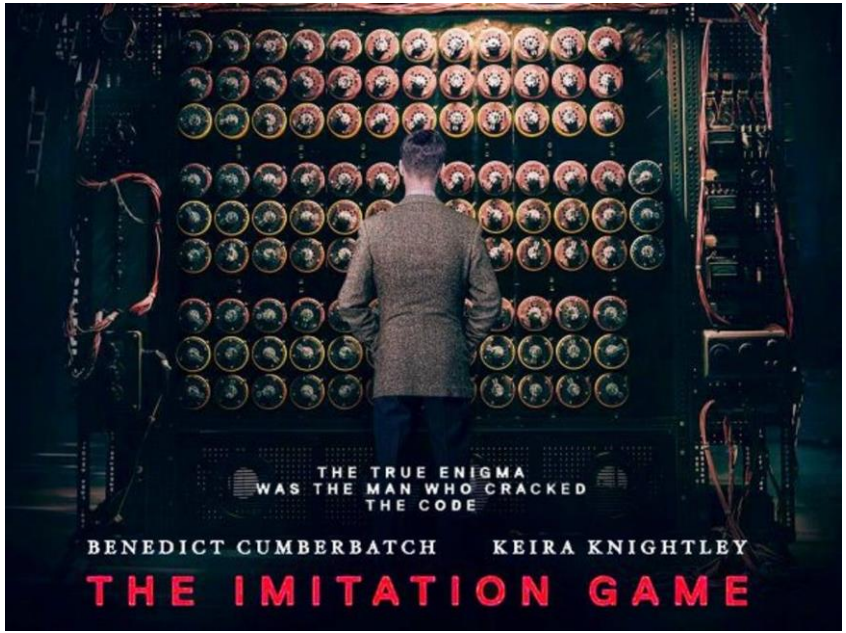
但新式數位身分證缺少這些特性!

*2千多萬筆個資外洩，多年後才因在暗網販售，被發現！**資料是舊的啦!***

加密無法確保資料永遠不會外流

雖然有加密 但已有前車之鑑
加密區資料仍有外流風險

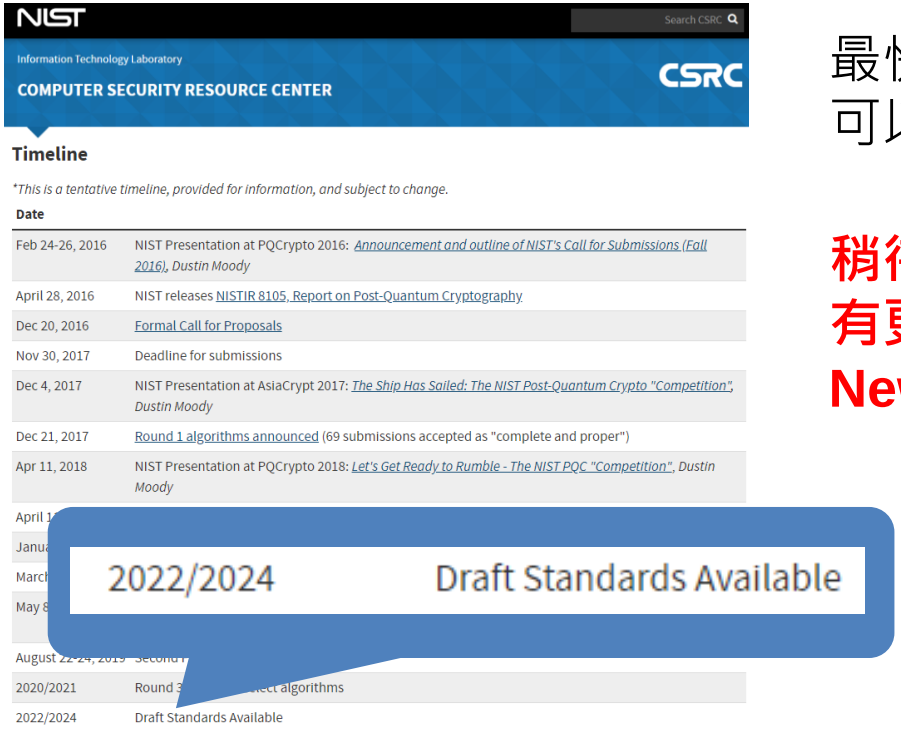
若加密被破解後



即便面臨德軍轟炸有犧牲英軍艦艇的壓力，只要有更大的目標，同盟國就算已經破解，Enigma machine 的加密方式，

也不會說出來!

量子電腦存在的威脅不容忽視



最快 2022 年後量子密碼標準問世，可以抵禦量子電腦的攻擊。

稍待 2 年
有更安全的標準問世
New eID 的發行

真的有那麼急嗎?

資料來源 – https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

資料數位化使風險提高

紙本身分證共 11 筆資料，
數位身分證公開區10筆資料

但 資料數位化後

1. 資料取得更為容易
2. 易於編輯與建立資料庫
3. 便於資料散布與流傳

你的隱私

他的方便

數位身分證資料讀取與遺失的風險

2014 年統計，該年度共有

44萬張
身分證遺失

使用更便利
- 會不會導致遺失的機會更多?

資料易編輯
- 會不會造就更多地下個資資料庫?

遺失數量多
- 會不會使得晶片更容易被破解?

人臉辨識是否真是種進步?

- 2019 年 5 月，舊金山首開先例，成為全球第一個禁用人臉辨識系統的城市
- 微軟刪除全球最大臉部辨識資料庫 MS-Celeb-1M，內含10萬個名人、1 千萬張照片 https://technews.tw/2019/06/13/ms-celeb-1m-was-deleted/
- IBM退出人臉辨識業務！CEO寫信疾呼：反對技術淪種族歧視幫兇 https://www.bnext.com.tw/article/58024/ibm-facial-recognition-george-floyd

人臉辨識是否真是種進步?

結　　語

- 資安難保證、風險可控管－**分散式的設計，本身就是安全的機制**
- The lesson from Alan Turing－**敵(他)國的駭客國家隊，破解密碼後，不會四處嚷嚷**
- 管理機制未完備，無法取得民眾的信任
- **『想知道是誰?』**是**一切邪惡的根本**

THANK YOU!

感謝 TWISC@NCTU 的協助