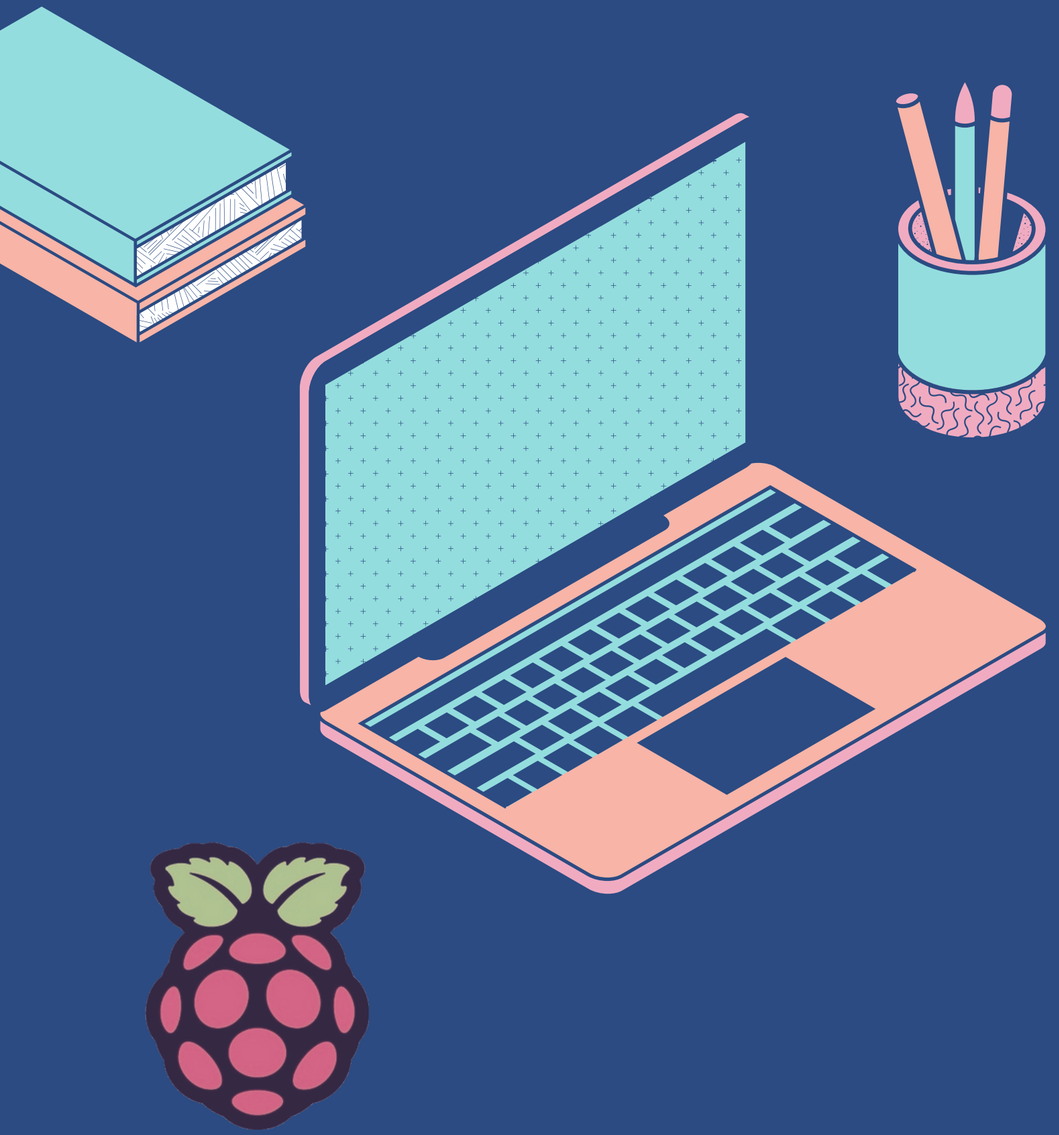
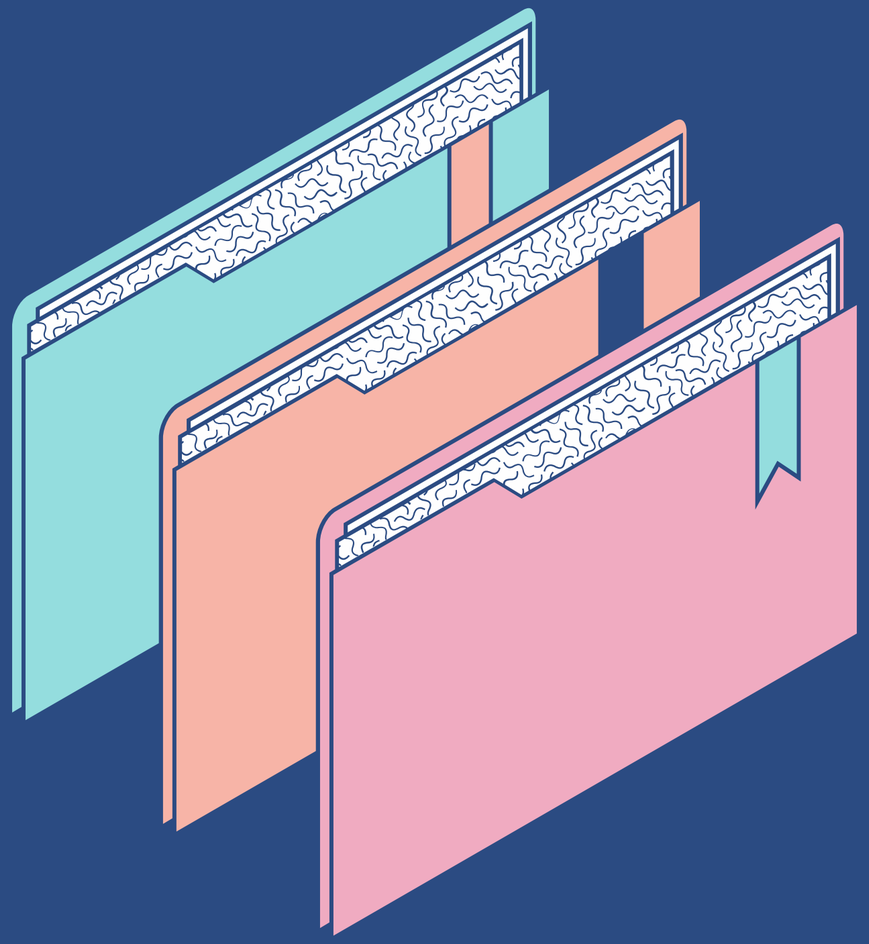


NM LAB FINAL PROJECT PROPOSAL

國軍弊案-
Rpi硬體錢包開發

組員：
b0990104翁瑋杉、b09901112洪牧白
b0990066謝承修、b09602017白宗民



Content

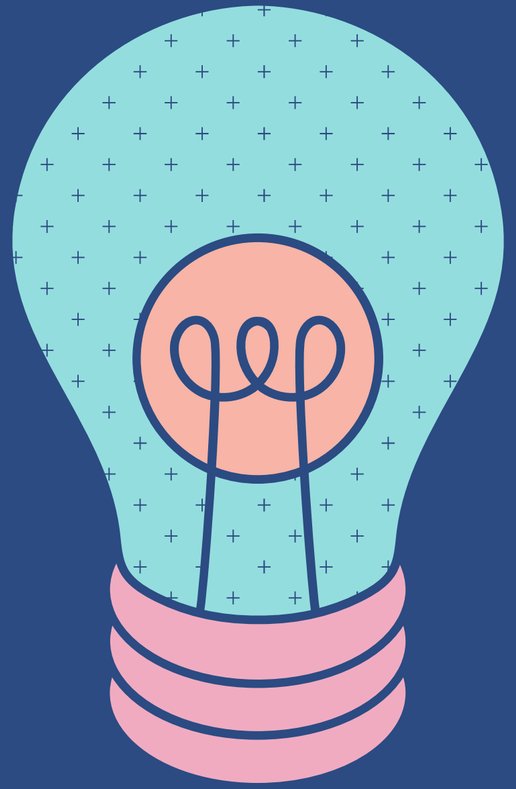
KEY TOPICS DISCUSSED IN
THIS PRESENTATION

- Introduction
- API Schema
- Flow Chart
- DEMO
- DID & VC Schema
- Questions to answer
- Technical Challenges and Solutions
- Reference
- Collaboration

Motivation

國軍防彈衣採購爆弊案！不肖廠商進中國製交貨賺1.7億價差 邱國正今早證實

因為最近國軍弊案頻傳的關係，導致國家機密外洩等等的國安問題頻傳。因此我們在這次的專題中打算使用Rpi上的TPM來建立並儲存DID，並透過VC的簽署來確保槍枝的交易流程都是合法、沒有被竄改過的，並且保證交易的資料的安全性。



API Schema

1. createRandomString:
    * input: none
    * output: string , ex: cff0ff4f7a744737722496f7db9d6277

2. generataKeyPair:
    * input: path to both priv.key, pub.key(set by myself) (eg. data/A/TPM/id_1.tss , id_1.pub)
    (.key files do not have to exist in advance)
    * output: public_key_str

3. Signing VC(using holder privkey):
    * input: json_file_str, privKey_path
    * output: signature_str

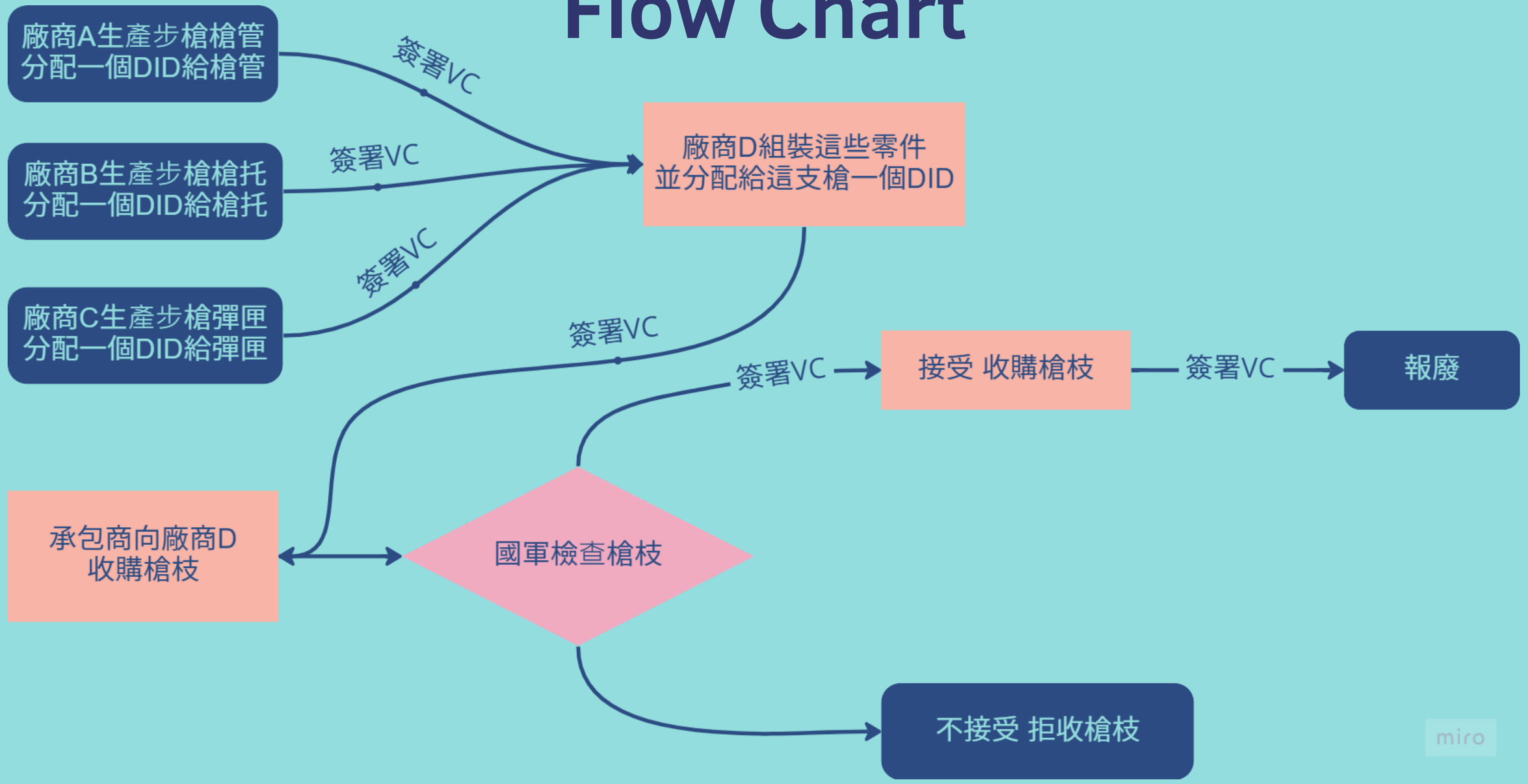
API Schema

4. Varify CV :
   * input: VC_str (exclude sign) , public_key_str , signvalue_str
   * output: True/False

5. storeVC:
   * input: str
   * output: none

6. getVC:
   * input: VC_str (exclude sign) , public_key_str , signvalue_str
   * output: True/False

Flow Chart



Demo

Flow Chart

廠商A生產步槍槍管
分配一個DID給槍管

廠商B生產步槍槍托
分配一個DID給槍托

廠商C生產步槍彈匣
分配一個DID給彈匣

被創建者：

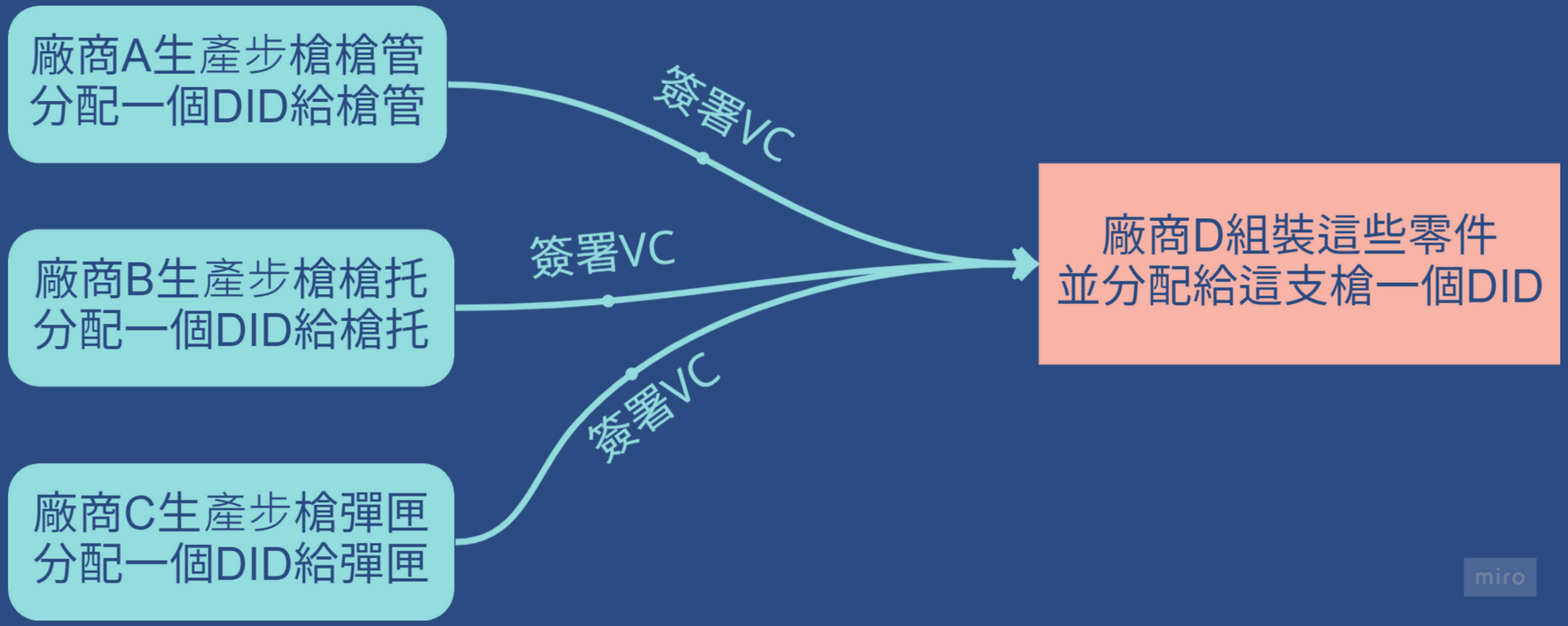
工廠A、B、C、D、國軍

承包商、國防部、國防工業基地局

建立組織 (產生DID)

1. 產生一個 public/private key pair
2. 每個組織都產生一個 DID doc
3. 將 DID doc 存入區塊鏈以及本地記憶體

Flow Chart



Issuer:
工廠A、B、C

Holder:
工廠A、B、C

Verifier:
工廠D

轉換所有權 (簽署VC)

1. Issuer (A,B,C)自己發這個VC並同時作為 holder
2. 產生一個 public/private key pair
3. Holder, Issuer 使用 RSA sign 去簽署此VC
4. 用 private key encrypt VC
5. Publish encrypted VC and VC public key
6. 這樣 Verifier (工廠D) 就可以用public key decrypt VC doc, 確認 VC合法性。

DID Schema

工廠、承包商、政府機關、槍枝及零件


```
{
  "@context": [ "https://www.w3id.org/did/v1" ],
  "id": "did:example:123456789_gun_stock",
  "publicKey": [
  {
    "id": "'did:example:123456789abcdefghi#keys-1",
    "type": "RsaSignatureAuthentication2022",
    "owner": "did:example:123456789_gun_stock",
  "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  } ],
  "authentication": [ {
        "type": "RsaSignatureAuthentication2022",
        "publicKey": "did:example:123456789abcdefghi#keys-1"
        } ],
  "service": [ {
        "type": "VerifiableCredentialService",
        "serviceEndpoint": "https://example.com/vc/"
        } ]
}
```

DID Schema

工廠、承包商、政府機關、槍枝及零件

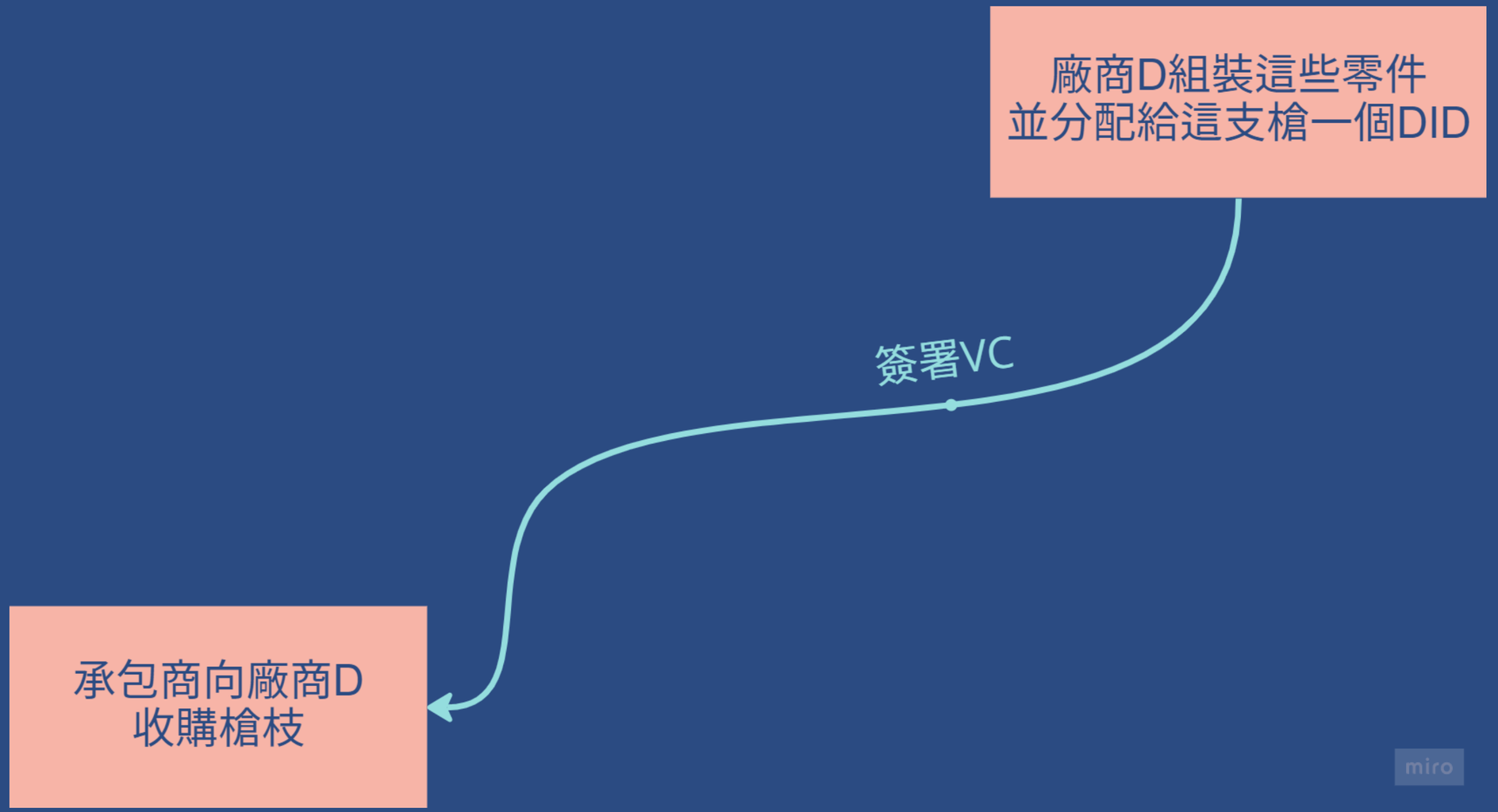

```
{
  "@context": [ "https://w3id.org/security/v1" ],
  "id": "did:example:123456789_A_transfer_B",
  "type": ["Credential","Ownership_transfer"],
  "issuer": "did:example:123456789_A_factory",
  "issued": "2010-01-01",
  "claim": {
        "seller": "did:example:123456789_A_factory",
        "buyer": "did:example:123456789_B_factory",
        "item": "did:example:123456789_gun_stock" },
  "revocation": {
        "id": "http://example.gov/revocation/738",
        "type": "SimpleRevocationList2022" },
  "signature": {
        "type": "LinkedDataSignature2022",
        "created": "2023-01-02 21:36:50.176441",
        "creator": "http://example.com",
        "domain": "json-ld.org",
        "nonce": "12345678",
        "signatureValue":"encryptionOfWholeDocument" }
}
```

VC Schema

槍管、槍托、槍彈匣


```
{
        "@context": [
                "https://wid.org/security/vI"
        ],
        "id": "did:example:123456789_A_transfer_B",
"action": "ownership_transfer",
        "item": "did:example:123456789_gun_stock",
        "claim": {
                "seller": "did:example:123456789_A_factory",
"buyer": "did:example:123456789_B_factory",
"owner":"s;lkgaj;lkg" },
        "revocation": {
                "id": "http://example.gov/revocation/738",
                "type": "SimpleRevocationList2022" },
        "signature": {
                "created": "2023-01-02 21:36:50.176441",
                "creator": "http://example.com"
        }
}
```

Flow Chart



Issuer:
國防工業基地局 (DIB)

Holder:
工廠D

Verifier:
承包商

組裝槍枝 (產生DID)

1. 產生一個 public/private key pair
2. 產生一個 DID document
3. 用 private key encrypt DID doc
4. 將 DID doc 存入區塊鏈以及本地記憶體

Issuer:
國防工業基地局 **(DIB)**

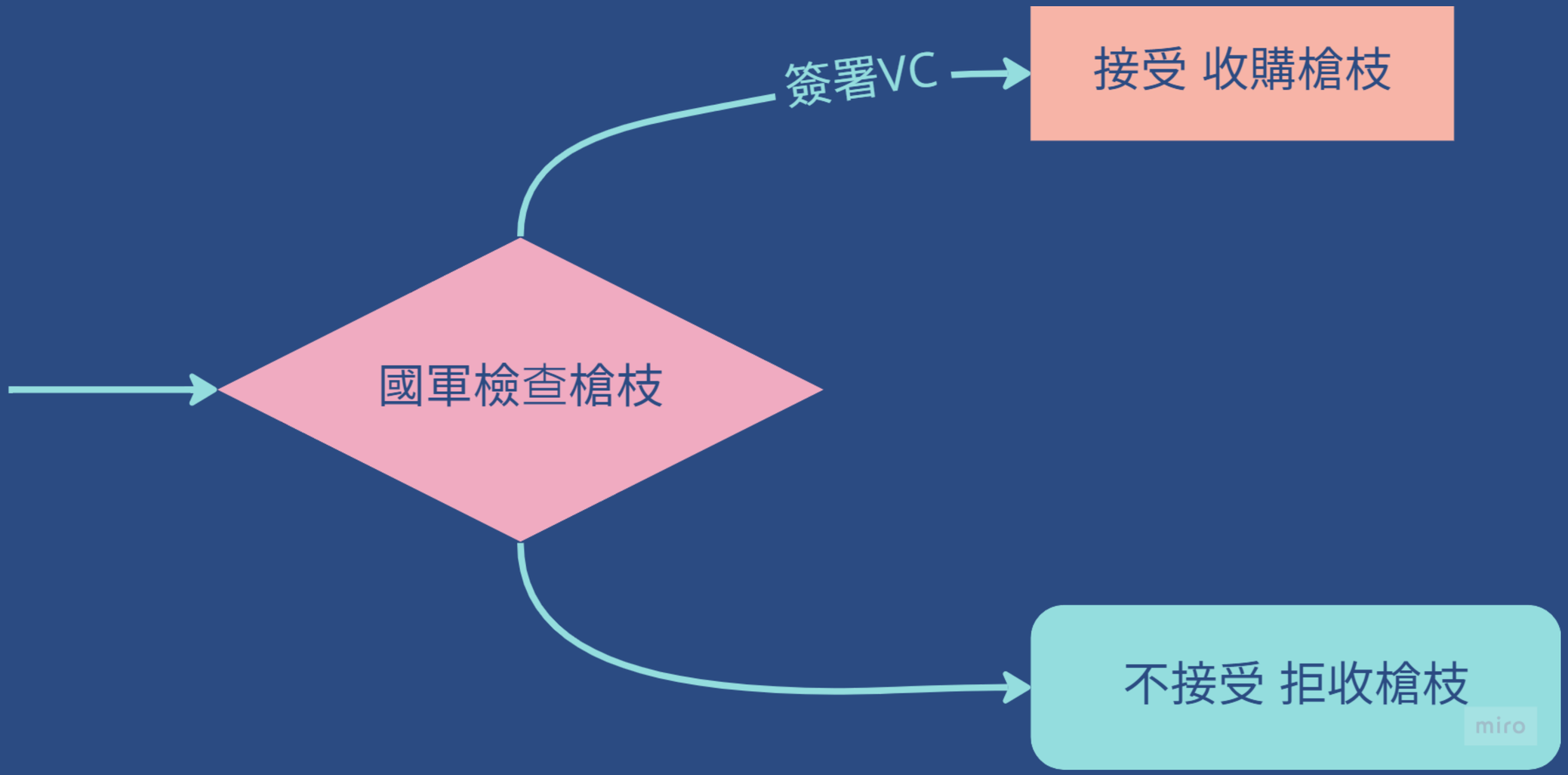
Holder:
工廠**D**

Verifier:
承包商

轉換所有權 (簽署VC)

1. Issuer (DIB) 發這個VC
2. Holder (工廠D) 持有這個VC
3. 產生一個 public/private key pair
4. Holder, Issuer 使用 RSA sign 去簽署此 VC
5. 用 private key encrypt VC
6. Publish encrypted VC and VC public key
7. 這樣 Verifier (承包商) 就可以用public key decrypt VC doc, 確認 VC 合法性

Flow Chart



Issuer:
國防部 **(MOD)**

Holder:
承包商

Verifier:
國軍

轉換所有權 (簽署VC)

1. Issuer (MOD) 發這個VC
2. Holder (承包商) 持有這個VC
3. 產生一個 public/private key pair
4. Holder, Issuer 使用 RSA sign去簽署此 VC
5. 用 private key encrypt VC
6. Publish encrypted VC and VC public key
7. 這樣 Verifier (國軍) 就可以用public key decrypt VC doc, 確認 VC docs 合法性

Flow Chart

Issuer:
國防部 (MOD)

Holder:
國軍

Verifier:
國防部 (MOD)

報廢槍枝 (撤銷DID)

1. 國軍找到此槍枝的 DID 文件並且刪除
2. 刪除這個 DID 所對應的 VCs

Issuer:
國防部 (MOD)

Holder:
國軍

Verifier:
國防部 (MOD)

報廢槍枝 (簽署VC)

1. Issuer (MOD) 發這個報廢槍枝的 VC
2. Holder (國軍) 持有這個 VC
3. 產生一個 public/private key pair
4. Holder, Issuer 使用 RSA sign 去簽署此 VC
5. 用 private key encrypt VC
6. Publish encrypted VC and VC public key
7. 這樣 Verifier (MOD)就可以用 public key decrypt VC doc, 確認 VC docs 合法性

Questions to answer

在物聯網裝置的生態系中物聯網的去中心化身份(DID)與可驗數位憑證(VC)長甚 麼樣?

以json檔的檔案型式儲存，如前頁中給出的範例。

一個IoT裝置的生命週期(lifetime)內會需要多少個DID?

一個IoT裝置的生命週期中只會有四個DID。

在物聯網裝置的生態系中，誰可以發布VC?

Issuer可以發佈及簽署VC。

Questions to answer

怎麼達到IoT的安全與隱私?

透過對稱式的加密來確保資料的安全。

有完成的物聯網裝置生命週期?

有。

假設的物聯網應用情境為何?

在此Project中假設了軍方採購軍火時需要保持資料的隱蔽性及安全性，同時確保在交易的過程中資料沒有外洩或被竄改，因此採用TPM來存儲DID以及VC，並且使用RSA sign的方式簽署VC來保證交易過程的安全。

Technical Challenges and Solutions

- VC及DID的具體簽署方式
  - 最後選擇使用RSA sign 而不是使用AK
- Issuer、Holder、Verifier之間的關係
  - 團體討論出每個動作的三角關係
- 弄清楚AK以及RSA sign的差異及使用情境
  - AK應該較特定簽署方式，並且經常用來簽署VC
- TPM的UI介面開發方式
  - 根據資料修改輸入格式以及增加更多可用GUI
- 每一次的公私鑰匙對的使用情境
  - 詢問chatGPT以及團隊討論
- Too long to be hashed
  - 簽小一點的資料
- 加解密的函式實作。
  - chatGPT 幫助了我們
- API的輸入輸出格式
  - 程式總監們討論出了各種API的對接方式

Reference

信賴運算 : http://d8888.blogspot.com/2005/07/blog-post_11226261315480909 7.html

加密演算法 : https://ithelp.ithome.com.tw/articles/10287338

ECDSA: https://steemit.com/cryptography/@oneleo/ecdsa-rfc6979

chatGPT : 如何利用DID簽署VC

chatGPT : 如何驗證VC

chatGPT : 其他所有問題

新聞 : 國軍防彈衣採購爆弊案！不肖廠商進中國製交貨賺1.7億價差 邱國正今早證實

GUI : https://github.com/Infineon/optiga-tpm-explorer/blob/python3_dev/Python_TPM20_GUI/tab1_setup.py

Collaboration

翁瑋杉：把TPM COMMAND 包成 PYTHON FUNCTION、主要脈絡發想

謝承修：撰寫README、撰寫使GUI BOTTOM能做到對應動作的程式、主要脈絡發想

白宗民：使用TPM並理解其中動作以協助上面兩位撰寫程式、REPORT內容、協助GUI

洪牧白：主要TPM GUI、主要REPORT格式及排版、海報製作、美編總監、協助FUNCTION及UI整合

Thanks fo listening

Issuer:
工廠A、B、C

Holder:
工廠A、B、C

Verifier:
工廠D

生產零件 (產生DID)

1. 產生一個 public/private key pair
2. 每個零件都產生一個 DID document
3. 用 private key encrypt DID doc
4. 將 DID doc 存入區塊鏈以及本地記憶體