數位憑證皮夾

TW DIW

數位憑證皮夾簡介

發表人

數位發展部

發表時間

115.01

章節

01	數位憑證皮夾簡介	03
02	發行端流程	11
03	驗證端流程	15
04	環境建置與資安架構	19
05	附件	21

TW DIW
數位憑證皮夾

01

數位憑證皮夾簡介

源起

現在

未來

- 多憑證整合
- 政府機關證件數位化
- 民營企業介接
- 簡單、安全、方便

數位憑證皮夾形象網站　https://www.wallet.gov.tw/zh-tw

驗證三角

發行端

使用者
加入電子卡

OID4VCI

持有端(使用者)

使用者
提供電子卡資料

OID4VP

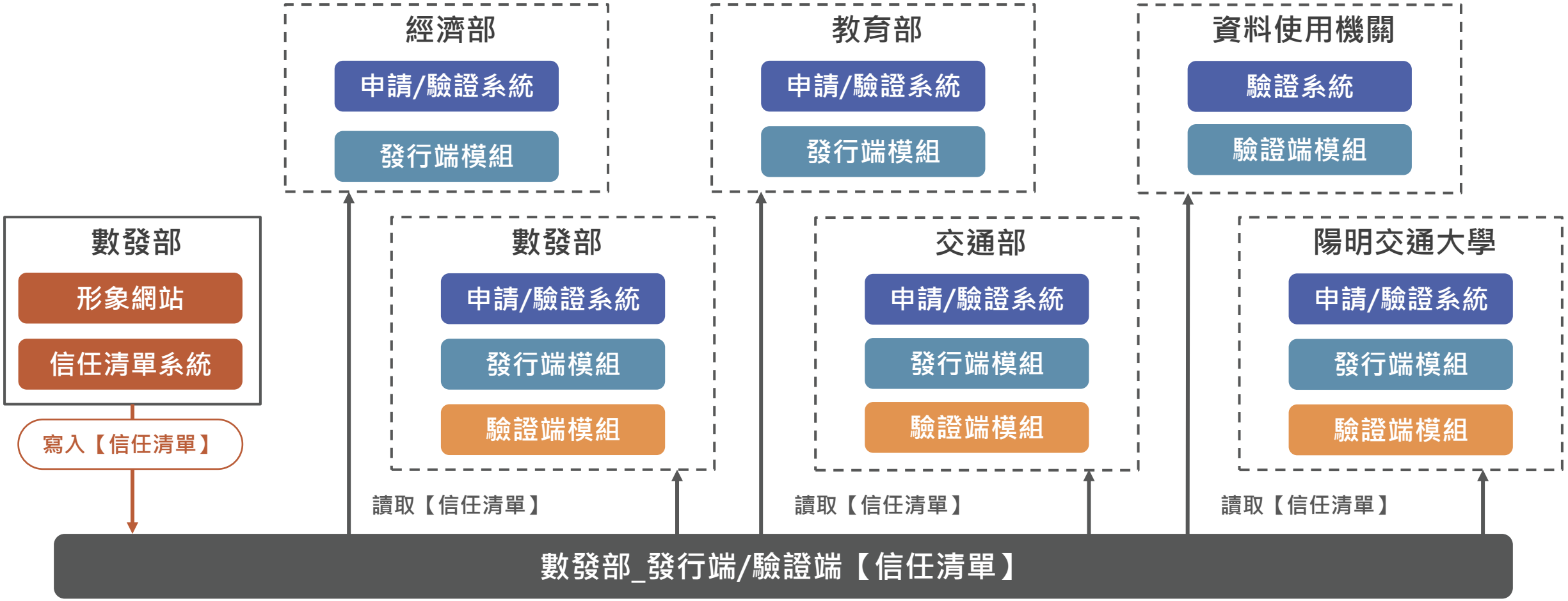
數位自主權 | 事實認同 | 安全與隱私保護 | 資訊安全 | 可信任服務清單 | 系統擴展性

未來可應用場景

 發行端	學校學生證	駕照	畢業證書	門號電子卡	訪客卡	工商憑證
 使用者	校園應用 畢業前 校園生活	租車應用 畢業旅行	求職應用 畢業後 投遞履歷	超商領貨 採購 面試物品	訪客管理 面試時 領取訪客證	申辦應用 企業主 辦理資料
 驗證端	學校門禁系統 學校借書系統	線上註冊 臨櫃租車	104、1111 人力銀行	統一、全家 超商	機關端 訪客系統	MyData

生態圈架構

- ✓ 每個政府機關或民間組織皆可同時為發行端及驗證端
- ✓ 只要於【信任清單】中的機關或組織都可進行發行及驗證



發行與驗證電子卡示意流程圖

A
[發行端]管理人員需先向數發部申請加入生態圈

B
使用者向[發行端]電子卡申請系統申請電子卡

C
[驗證端]管理人員需先向數發部申請加入生態圈

D
使用者將資料提供給[驗證端]業務驗證系統

使用者

B1 申請電子卡

B2 電子卡加入皮夾

D1 提供資料給驗證端(自主揭露)

發行端管理人員

A1 申請成為發行端

發行端
(ex.公路局)

電子卡申請系統

發行端模組

A2 寫入信任清單

D3 (定時)下載電子卡【狀態清冊】

驗證端
(ex.租車公司)

業務驗證系統

D4 驗證電子卡有效性

驗證端模組

D2 (定時)查詢發卡單位是否有在【信任清單】

C1 申請成為驗證端

C2 寫入信任清單

驗證端管理人員

數發部_發行端/驗證端【信任清單】

相關資源說明

01	數位憑證皮夾形象網站	https://www.wallet.gov.tw/zh-tw
02	沙盒系統帳號與組織申請	https://wallet.gov.tw/apply/applyAccount.html
03	發行端沙盒系統	https://issuer-sandbox.wallet.gov.tw/
04	驗證端沙盒系統	https://verifier-sandbox.wallet.gov.tw/
05	沙盒發行端 Swagger API	https://issuer-sandbox.wallet.gov.tw/swaggerui/
06	沙盒驗證端 Swagger API	https://verifier-sandbox.wallet.gov.tw/swaggerui/
07	情境模擬展示網站	https://demo.wallet.gov.tw/

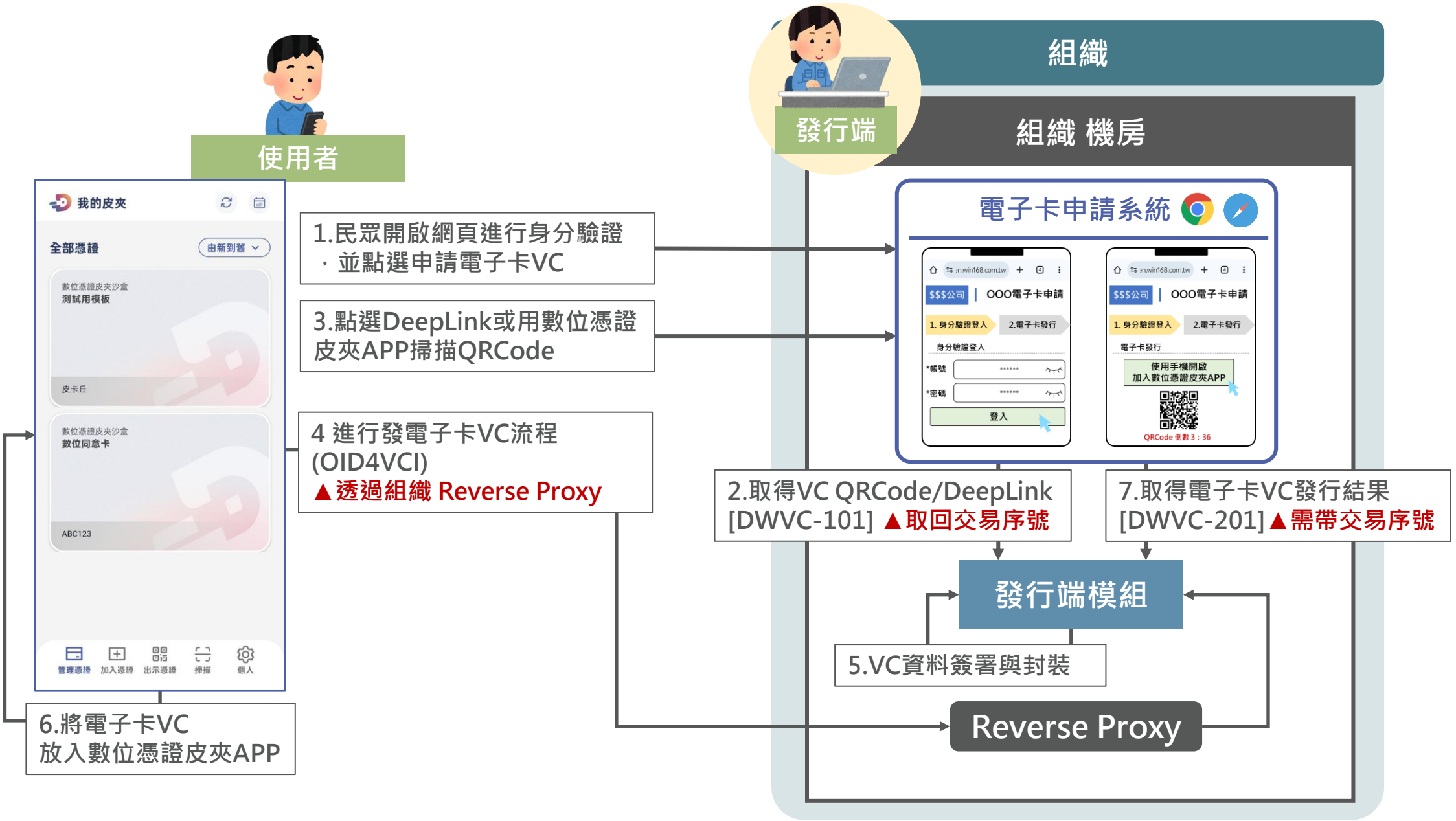
TW DIW 數位憑證皮夾

02

發行端流程

發行端發行電子卡流程

▼所有環境皆在組織內部



發行端組織需執行項目

▼紅字為發行端所需執行項目

發行端模組

- 安裝：由數位發展部提供(Docker、WAR、Java 原始碼)，部署在參與組織的主機
- 6 封裝卡片，讓使用者的數位憑證皮夾APP加入卡片

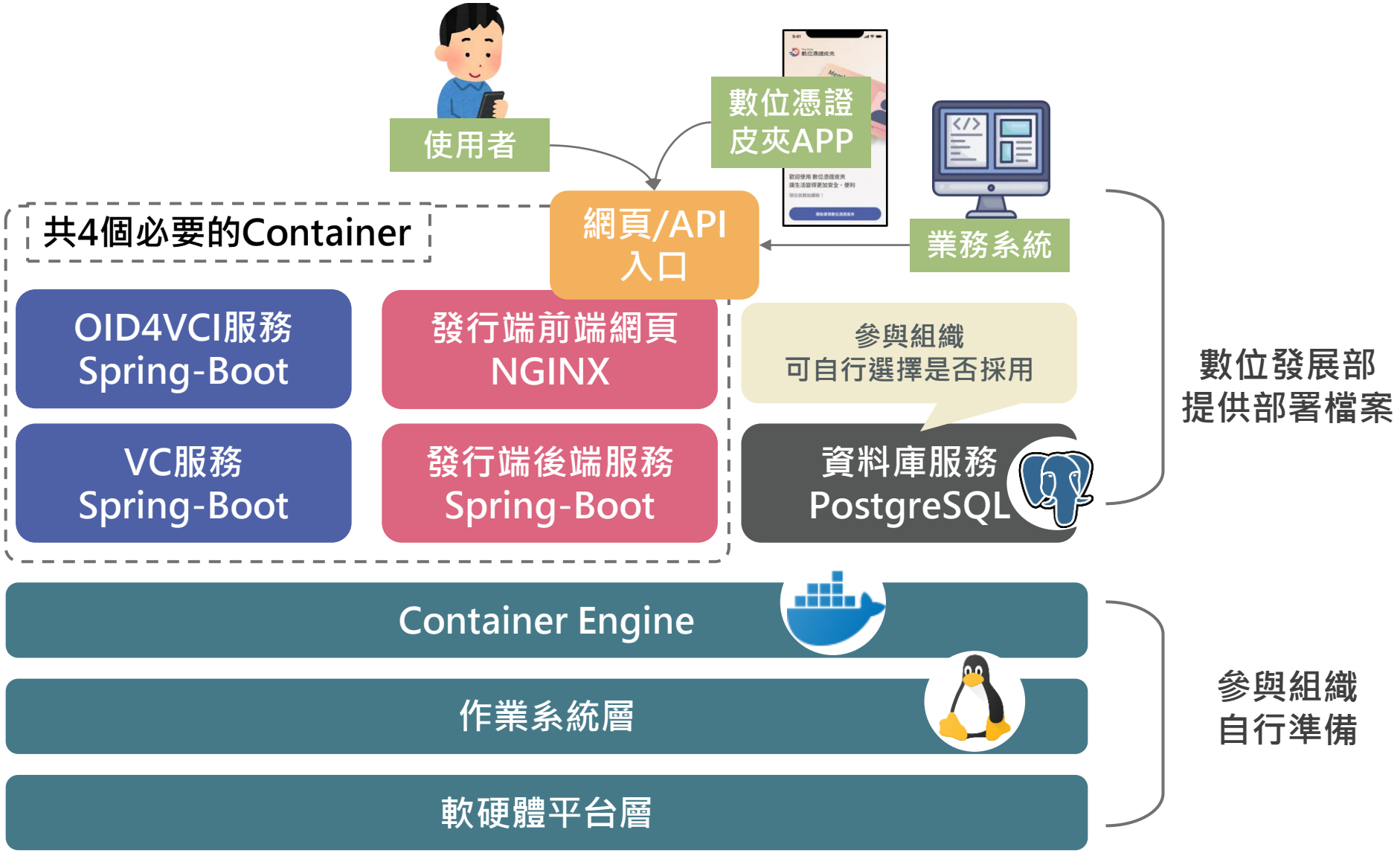
發行端 電子卡申請系統

- 開發發行電子卡功能
  - 1 身分驗證與記錄民眾申請的資料
  - 2 呼叫發行端模組API，取得QR Code [DWVC-101]
  - 3&4&5 民眾掃描QRCode，傳送Nonce值至發行端服務
  - 7 取得發行結果 [DWVC-201]
- 取消或撤銷電子卡功能
  - 對發行端模組呼叫廢止的API [DWVC-301]

記錄民眾申請資料的表格範例	
KEY	VALUE
NONCE	xokukfien
登入帳號	wahaha@abcmail.com
申請卡片	卡片詳細資料

電子卡VC資料 範例	
欄位	資料
姓名	王小明
生日	2000/01/01

發行端模組架構


使用者
數位憑證
皮夾APP
業務系統
共4個必要的Container
網頁/API
入口
OID4VCI服務
Spring-Boot
發行端前端網頁
NGINX
參與組織
可自行選擇是否採用
VC服務
Spring-Boot
發行端後端服務
Spring-Boot
資料庫服務
PostgreSQL
數位發展部
提供部署檔案
Container Engine
作業系統層
軟硬體平台層
參與組織
自行準備

TW DIW 數位憑證皮夾

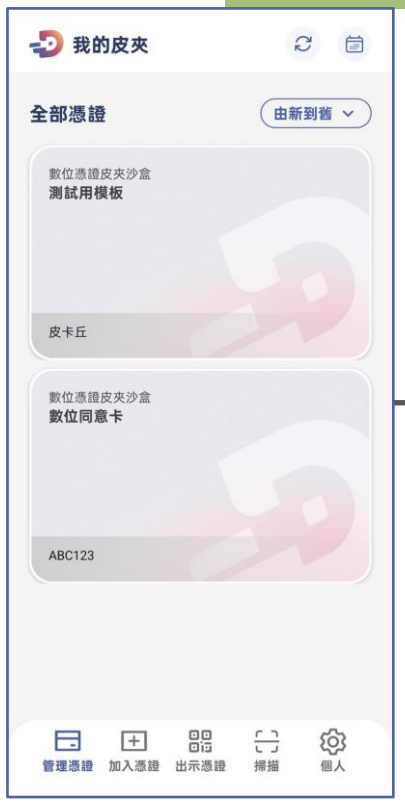
03

驗證端流程

驗證端資料驗證流程

▼所有環境皆在組織內部

使用者



2.使用數位憑證皮夾APP掃描QRCode

3. 進行驗證流程
[OID4VP]
▲需帶交易序號
▲透過組織 Reverse Proxy

組織

組織 機房

驗證端

驗證端業務系統

1. 取得申請VP QRCode/Deep-link
[DWVP-101]▲需帶交易序號

4.驗證VP資訊是否成功
[DWVP-201]

驗證端模組

Reverse Proxy

驗證端組織需執行項目

▼紅字為驗證端所需執行項目

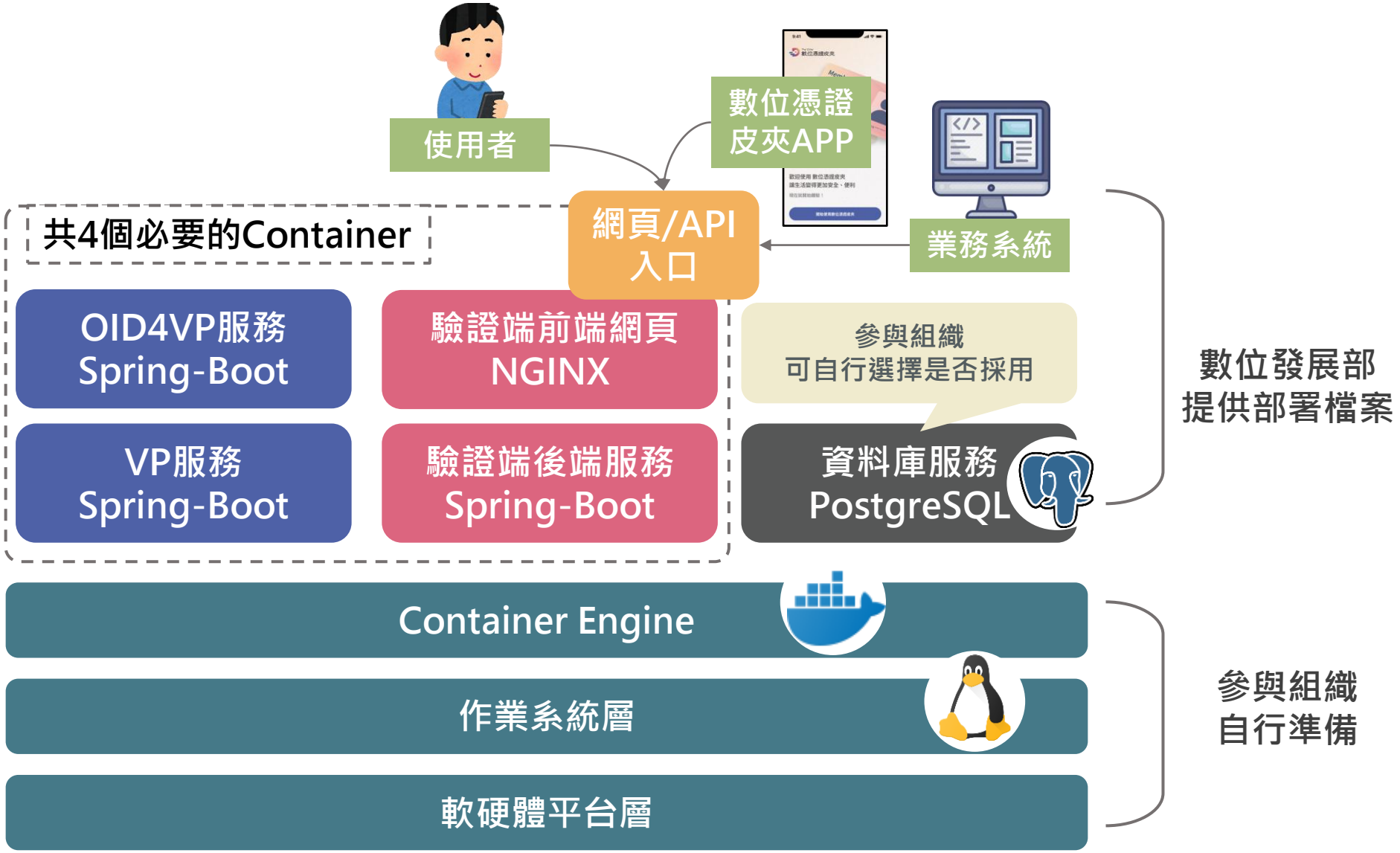
驗證端模組

- 安裝：由數位發展部提供(Docker、WAR、Java 原始碼)，部署在參與組織的主機

驗證端 業務驗證系統

- 開發接收使用者提供資料的網頁
  - 1 呼叫驗證端模組取得QR Code [DWVP-101]
  - 2&3 民眾開啟數位憑證皮夾APP掃描QR Code，將資料傳送至「驗證端模組」
  - 4 取得驗證結果[DWVP-201]

驗證端模組架構


使用者
數位憑證
皮夾APP
業務系統
網頁/API
入口
共4個必要的Container
OID4VP服務
Spring-Boot
驗證端前端網頁
NGINX
參與組織
可自行選擇是否採用
VP服務
Spring-Boot
驗證端後端服務
Spring-Boot
資料庫服務
PostgreSQL
數位發展部
提供部署檔案
Container Engine
作業系統層
軟硬體平台層
參與組織
自行準備

04

環境建置

組織伺服器主機需求


✓ 作業系統建議為Linux(需包含 Docker相關套件)

✓ 所有服務以Docker方式運行，數發部開發團隊將提供安裝手冊與Shell Script與讓參與組織可自行安裝與啟動

VM 規格

- Reverse Proxy VM : 2 Core、4GB RAM、200GB

- 應用伺服器(DB)虛擬機規格：4 Core、16GB RAM、 (UAT)300GB/ (PROD)300GB ，需可連線至Internet 指定位置
- 部署：發行端服務(含後台)、驗證端服務(含後台)、獨立發行端前端網頁

全機房落地

UAT 環境 (2台)

- Reverse Proxy VM * 1
- 應用伺服器(DB)虛擬機規格 (UAT) * 1

PROD 環境 (4台)

- Reverse Proxy VM * 2
- 應用伺服器(DB)虛擬機規格 (PROD) * 2 (可依實際環境架構，搭配 SLB 設備分流至 Reverse Proxy)

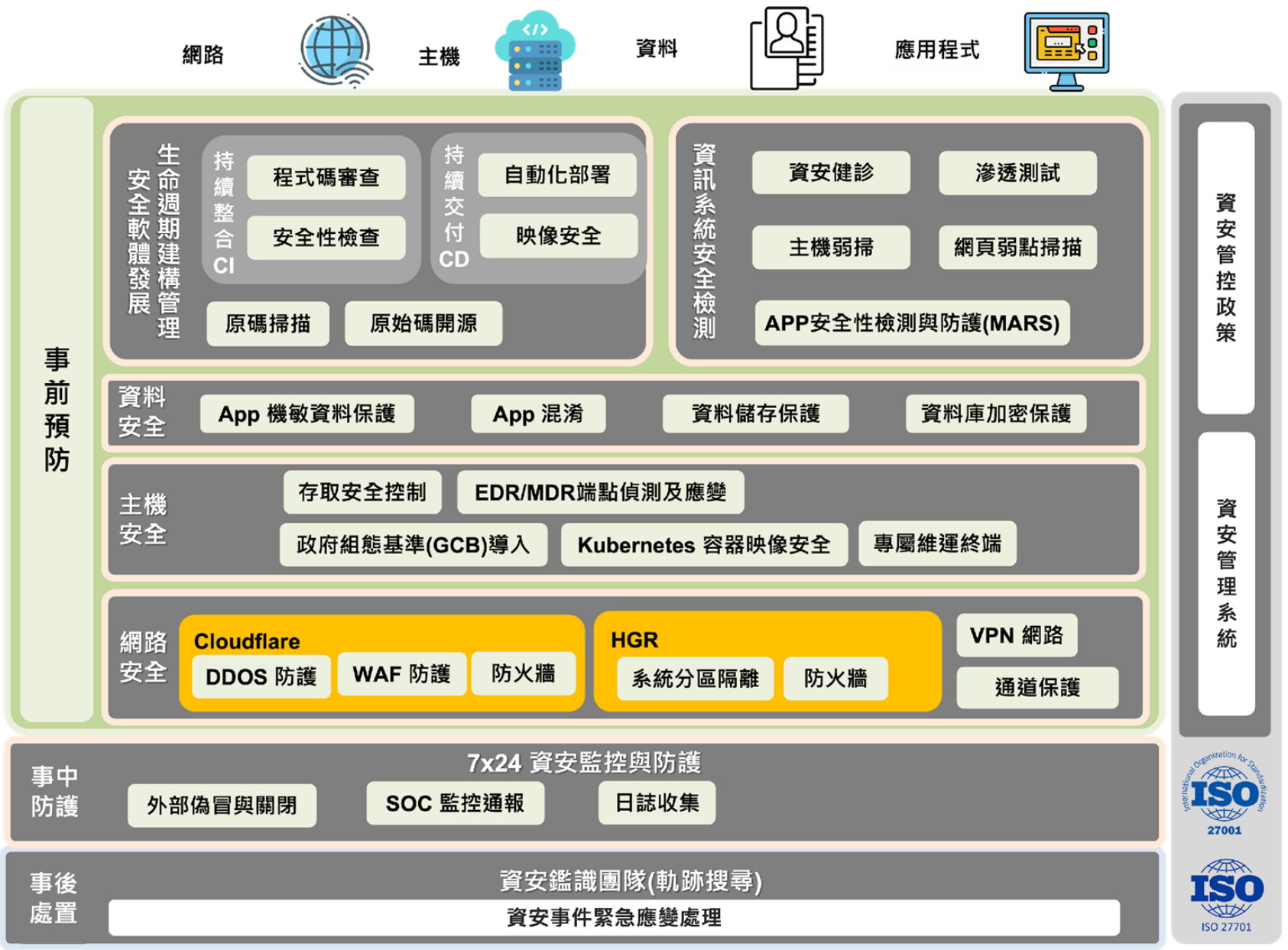
資訊安全架構

廣度防護三階段

- 事前建立安全防禦與安全檢測
- 事中做好嚴密安全監控並進行外部偽冒偵測與關閉達到橫向聯防
- 事後快速應變並以數位鑑識降低災害損失

縱深防禦四構面

- 整合Cloudflare，達到資訊安全、快速與高效率的三重效果
- 採用紅隊演練手法，補足傳統滲透測試容易忽略之邊界防禦
- 藉由內稽內控機制，確認各項控制項均已落實執行
- 導入ISO 27001資訊安全管理標準、ISO 27701 隱私管理標準



數位憑證皮夾_聯絡窗口

01 KPMG - 張奕虹 經理 ---- caitlinchang@kpmg.com.tw

02 KPMG - 康雲翔 顧問 ---- casperkang@kpmg.com.tw

TW DIW
數位憑證皮夾

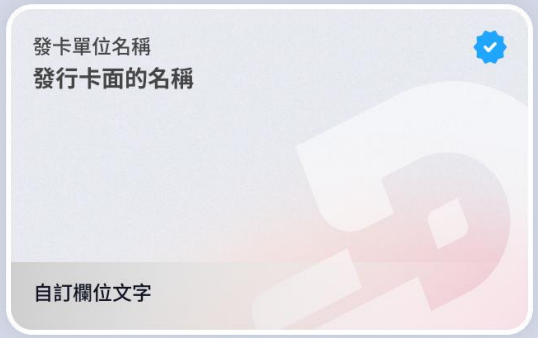
05

附件

信任清單與狀態清冊說明

信任清單

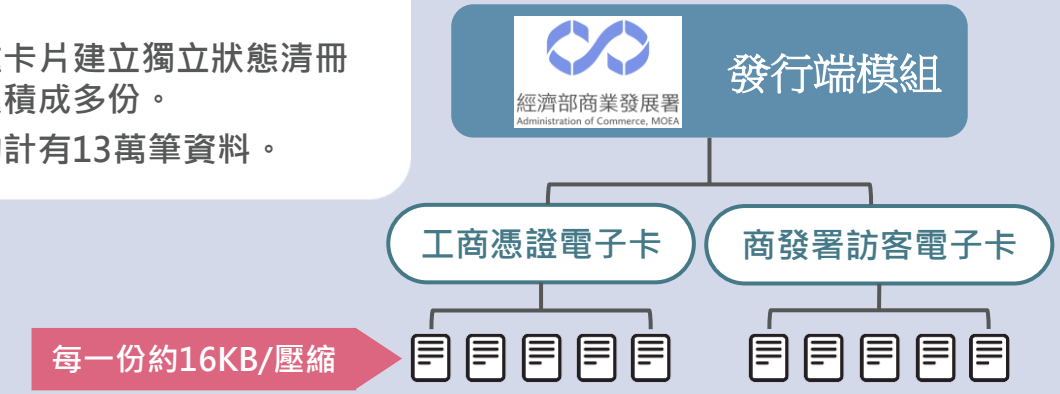
- **加入卡片→**
  - ✓ APP中卡片會有藍勾勾。



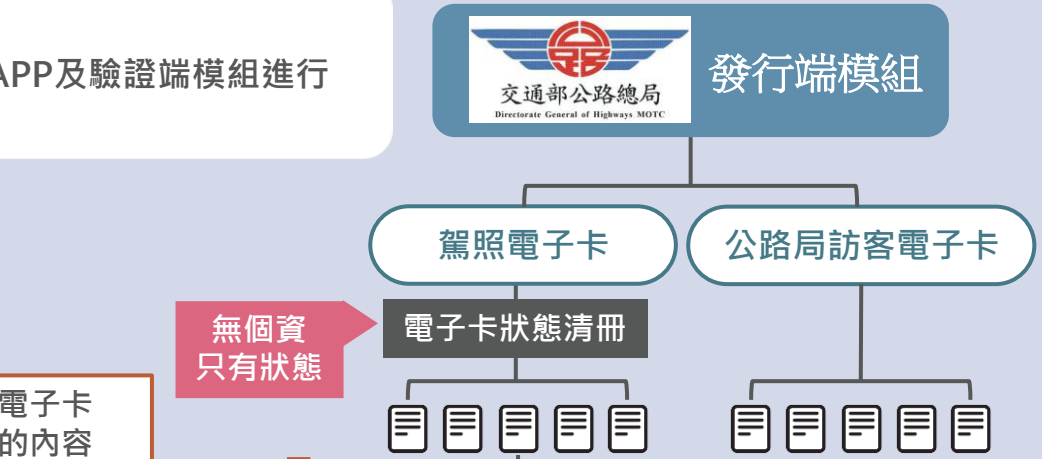
- **卡片驗證**
  - ✓ 若驗證單位不在信任清單中，APP有提示訊息，使用者可自行判斷是否將個資傳遞給非受信任的單位(非強制限制) 。

狀態清冊

- **發行時規則**
  - ✓ 發行端模組為每種卡片建立獨立狀態清冊，並依發卡總量累積成多份。
  - ✓ 每一份狀態清冊約計有13萬筆資料。



- **驗證時機制**
  - ✓ 狀態清冊會提供給APP及驗證端模組進行驗證時使用。



APP下載

立即下載
數位憑證皮夾 APP

GET IN ON Google Play

支援有 NFC 功能
且 Android 10 以上(含)

Download on the App Store

支援 iPhone XS 系列以上
且 iOS 15.0 以上(含)

申請加入發行端/驗證端流程

步驟 1
申請單位填寫
加入【發行端/驗證端】
申請單，將文件交付予
數位發展部並完成審查

步驟 2
數位發展部審查完成並通過後
，回覆申請單位審核結果
及模組基礎網址

步驟 3
發行端/驗證端模組申請系統
申請單位進入
發行端/驗證端模組申請系統
，進行申請作業

步驟 4
下載安裝包
申請完成，收到電子郵件
(內含一組Access Token)
前往「安裝包」下載連結
，進行安裝作業

步驟 5
發行或驗證端安裝包安裝完成

步驟 6
發行端/驗證端模組
使用工商憑證/XCA/GCA憑證
及填入Access Token
，進行DID註冊

步驟 7
DID註冊成功

步驟 8
組織LOGO上傳
可自由選擇
上傳組織LOGO顯示
在數位憑證皮夾形象網站

發行端模組API流程圖

發行端

電子卡申請系統

▲發行端提供

02 驗證使用者身分

05 建立此次交易的『唯一序號』與登入者資訊綁定

08 提供QRCode或DeepLink給電子卡申請畫面

06 OOO電子卡資料、VCID等資訊

07 QRCode或DeepLink

發行端模組 #容器化服務 #OID4VCI

▲數發部提供部署發行端

13 依據OOO電子卡資料封裝成 VC 電子卡

01 「使用者」登入「發行端OOO電子卡申請頁面」(執行身分驗證)

03 回傳身分驗證結果

04 「使用者」點選申請「OOO電子卡」

09 回傳QRCode或DeepLink

10 「使用者」使用數位憑證皮夾APP掃描QRCode或點選DeepLink

可定時詢問QRCode是否有被掃描了，請參考 [DWVC-201]：/api/credential/nonce/{nonce_id}

顯示QRCode，請參考 [DWVC-101]：/api/qrcode/data

12 啟動 VC 申請程序 (OID4VCI)

14 回傳VC 電子卡

若發行端要【撤銷】此卡片，請參考 [DWVC-301]：/api/credential/{cid}/{action}

使用者

電子卡申請畫面

▲發行端提供

開啟

TW DIW 數位憑證皮夾 APP

11 取得QR Code內URL並連線至發行端模組

15 將OOO電子卡儲存於數位憑證皮夾APP

比對 → 信任清單

驗證端模組API流程圖

使用者

業務驗證畫面

▲驗證端提供

開啟

TW DIW 數位憑證皮夾 APP

08 取得QR Code內URL並連線至驗證端模組

比對 → 信任清單、VC狀態、VC效期等

11 依電子卡類別與欄位，由使用者自主揭露欲同意的資料

01 「使用者」線上申辦業務並點選透過數位憑證皮夾提供「OOO電子卡」資料

06 回傳QRCode或DeepLink

07 「使用者」使用數位憑證皮夾APP掃描QRCode或點選DeepLink

顯示QRCode，請參考 [DWVP-01-101]：api/oidvp/qrcode

取得民眾自主上傳的資料，請參考 [DWVP-01-201]：/api/oidvp/result

09 傳送『唯一序號』

10 回傳需要的VC 電子卡與其欄位

12 傳送「使用者」自主揭露的VC 電子卡與其欄位

14 回傳資料驗證結果

驗證端

業務驗證系統

▲驗證端提供

02 建立此次交易的『唯一序號』

05 提供QRCode或DeepLink給線上業務申辦系統畫面

03 『唯一序號』、VPID

04 QRCode或DeepLink

驗證端模組 #容器化服務 #OID4VP

▲數發部提供部署驗證端

13 進行驗證

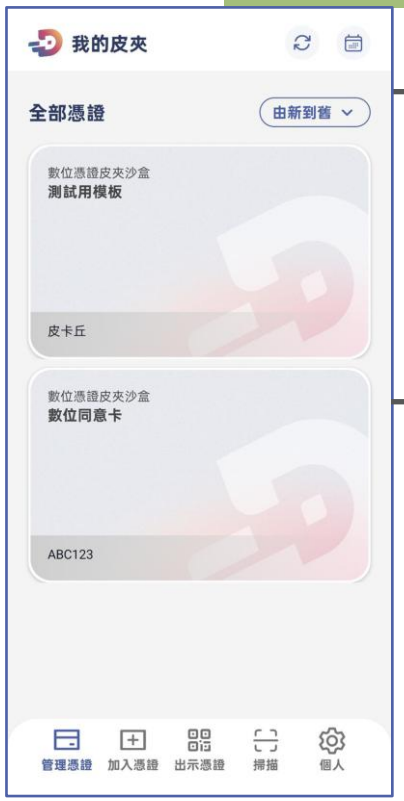
比對 → 信任清單、VC狀態、VC效期等

驗證端資料驗證流程(靜態QRCode)

▼所有環境皆在組織內部

使用者

掃描靜態 QRCode



1.使用數位憑證皮夾APP掃描
靜態VP QRCode

2.呼叫驗證端業務系統產生驗證VP Deep link
[DWVP-02-101]

組織

組織 機房

驗證端

▼參與單位需自行開發

驗證端後端服務系統

[DWVP-02-101、 DWVP-02-201]

3.取得申請VP QR Code/Deep link
[DWVP-01-101]
▲需帶交易序號

5. CallBack VP 驗證結果與取得資訊
[DWVP-02-201]傳送 VP 取得資料

驗證端模組

Reverse Proxy

4. 進行驗證流程
[OID4VP]
▲需帶交易序號
▲透過組織 Reverse Proxy

謝謝聆聽

Sincerely