

教育部大專院校數位證書建置試辦計畫

計畫介紹、系統說明、配合事項、計畫期程、未來規劃

計畫主持人：成功大學莊坤達副教授 / 舒宇宸副教授

計畫負責人：呂紹民 / smlu@netdb.csie.ncku.edu.tw

全國大專院校數位證書試辦計畫

計畫概要說明



計畫緣起

因應數位化時代、國際人才需求、學位證書真偽檢驗需求大增，為提供快速便利可靠之數位畢業證書機制，教育部於 108 學年度請成功大學建置全國大專院校數位證書發證/驗證系統。

本發證系統生成含有 metadata 的 PDF 文件，搭配 SHA3 家族的 SHA256 的 Hash 計算，並以 HashChain 方式進行驗證、偽造等確認。

本證書驗證系統提供全國合作大專院校之學位證書驗證，於 109 學年度開放使用，方便業界快速檢驗數位學位證書之真偽性。

各校作業程序

各校行政流程處理

- 統一數位證書樣式
- 數位證書發放流程確認
- 校內行政宣導、問題確認

各校系統串接

- 畢業學生名單資料串接 API (JSON)
- 各校畢業證書 PDF (建議基於畢業列印系統生成)
- 校內發證權限、憑證等相關權限管理

全國大專院校數位證書試辦計畫

數位證書系統設計原則



數位包容

- 創造人人公平的數位機會
- 減少數位落差，降低數位發行所需成本
- 提升學校自主性，減少商業可能限制

數位治理

- 建立以資料為核心、需求導向的智慧校園
- 整合服務功能，創新智慧服務
- 開放資料透明，極大化加值應用

數位參與

- 打造初期發證系統，方便各校導入使用
- 提升數位應用能力，衍伸後續加值服務
- 逐步協助數位轉型，優化校內行政流程



The screenshot shows the '教育部數位證書發證系統' (Ministry Digital Certificate Issuance System) interface. It includes a search bar for student IDs, a '數位證書申請狀態' (Digital Certificate Application Status) section with buttons for '中文證書' and '英文證書' (both marked '未申請' - Not Applied), and a '畢業生資訊' (Graduate Information) section. The graduate information is divided into '個人資料' (Personal Information) and '修業內容' (Degree Program Content). The personal information for '陳小明' (Chen Xiaoming) includes ID 'P83774662' and birthdate '1990/01/01'. The degree program content shows '畢業學校' (Graduation School) as '國立成功大學' (National Cheng Kung University) and '畢業系所' (Graduation Department) as '資訊工程學系' (Department of Information Engineering).

個人資料	
姓名	陳小明
學號	P83774662
出生日期	1990/01/01
電子信箱	P83774662@gs.ncku.edu.tw ming123@gmail.com

修業內容	
畢業學校	國立成功大學
畢業系所	資訊工程學系
其他資訊 (雙主修/輔系/不分系)	輔修：企業管理系 FinTech金融科技學分學程

數位證書發證系統

架設於各學校，供學校「發放」數位證書使用

系統功能

- 中文畢業證書
- 中文畢業證明書
- 中文畢業證書更名
- 英文畢業證書
- 英文畢業證明書
- 畢業證書發放查詢

初次發證 API (供各校串接校內系統，批次發證使用)

- xxx.yyy.zzz：各校發證IP/Domain name
- ID：為畢業學生之學號
- Chinese/English：發放證書的語系差異

(範例：[https://xxx.yyy.zzz/issue/?ID=\[學號\]](https://xxx.yyy.zzz/issue/?ID=[學號]) & language=[Chinese/English]/)



數位證書驗證系統

架設於教育部，供各界「驗證」數位證書

<https://dcert.moe.gov.tw/>



認證成功

此數位證書已受教育部與大專院校認證



認證失敗

此數位證書未受各大專院校認證

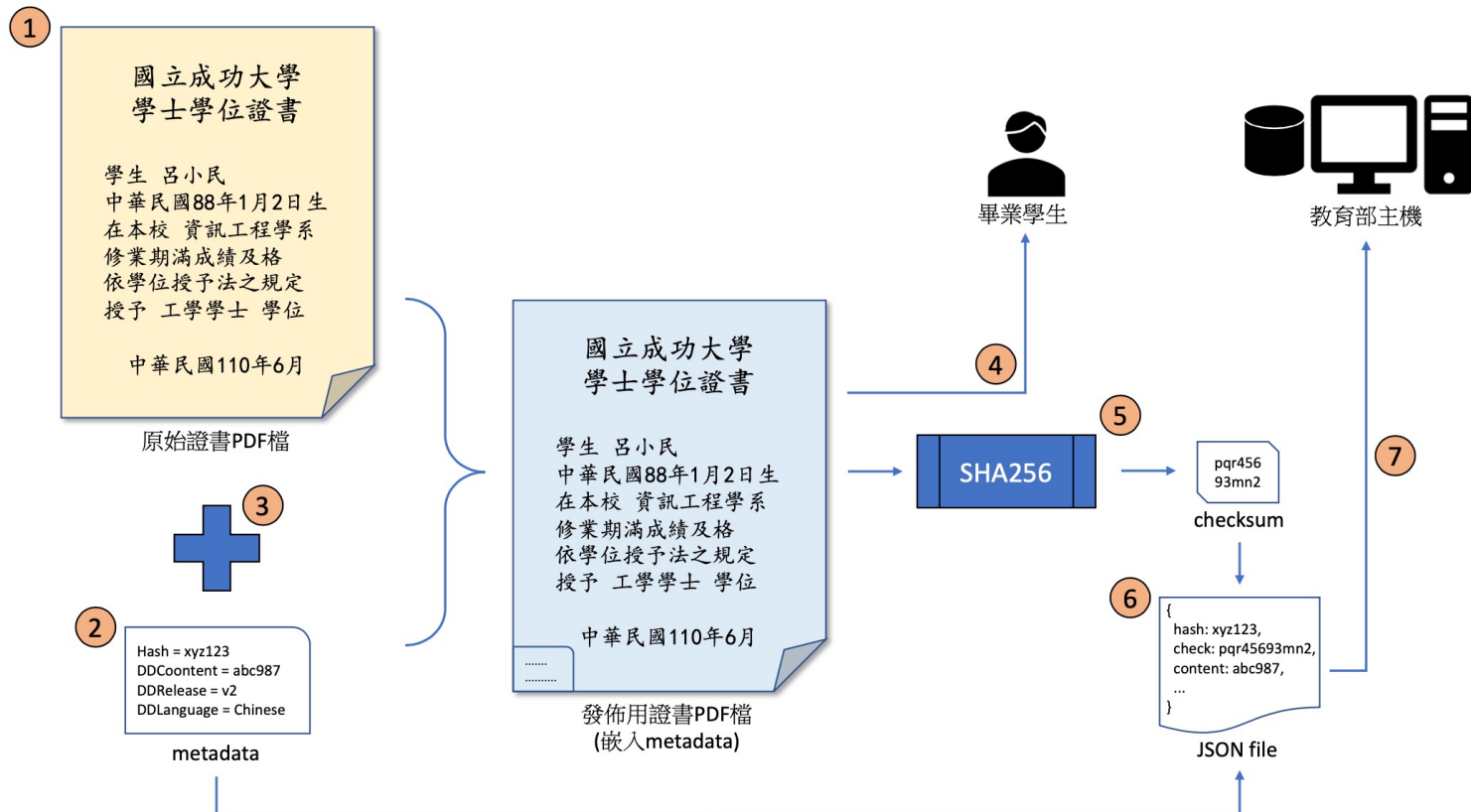


認證警告

此數位證書已非最新版本，
請向證書提供者、發證校方確認

各學校應確保 (1) ~ (4) 證書資料正確性

數位證書系統架構



行政義務、技術開發義務、合作權利說明

各合作學校權利與義務



學校合作義務

行政事項

- 各校應派出具執行能力之教務同仁、技術同仁各一名，作為本計畫合作對口
- 各校應有義務妥善保存發證主機內部之畢業學生個人資料、已發證數位證書
- 各校應配合未來教育部之行政稽核事項，以確保校內發證品質
- 未經教育部或本團隊同意，不得將系統原始碼自行對外釋出給其他學校或廠商等

學校合作權利

- 參與學校有權取得本計畫最新之發證系統與文件，並符合教育部所訂定之數位證書要求
- 參與學校有權取得本計畫提供之諮詢服務，以建立校內發證系統

技術開發

- 各校發證主機應設定基本資安防護，並應設定排程將相關資料定期備份並規劃異地備份機制
- 各校應具備能力自行開發符合校內學制、行政需求之「Raw PDF 串接程式」
- 各校應具備能力自行開發校內之「學生畢業資料串接程式」
- 各校應妥善維護發證主機、維持發證系統運作

7~8月基礎設施建置、9~10月系統安裝整合、11~12月測試宣傳 數位證書計畫建置時程



參考「數位證書合作標準流程」文件 計畫合作步驟



1

各合作學校決議參與本計畫，並回覆高教司公文以確認參與

本次會議後，請未確認之學校最晚於 7/30 前告知是否參與本計畫
後續會議紀錄將行文至各學校，請參與學校回函教育部以示正式加入

2

學校準備數位學位發證所需之資料

請學校準備資料串接 API、證書 PDF 檔案、發證主機、公開 IP 與 Domain Name

3

發證系統安裝包建置、系統測試

相關資料準備齊全後，計畫團隊將提供系統安裝包、使用文件
並安排工程師教學應如何進行系統介接，並提供各學校技術諮詢服務

系統營運事宜、學生個資保護、計畫相關費用、合作學校義務、計畫合作期程

計畫常見問題



系統營運事宜

- 發證系統由各學校自行維護、營運
- 驗證系統由未來教育部委派管理單位維護
- 計畫系統原始碼將提交教育部保存、管理

計畫相關費用

- 本計畫合作學校需自行負擔校內主機搭建成本 (系統主機、SSL憑證等)
- 本計畫無需額外負擔任何費用

學生個資保護

- 教育部僅儲存證書 Hash 值、metadata 檢核資料，並不紀錄學生個資資訊
- 學生個資僅儲存於各校發證主機中，由各校自行管理、維護

合作學校義務

- 各校應派行政 / 技術人員各一名參與本計畫
- 各校應具備足夠資訊能力建置本發證系統
- 其他權利義務細節請參考簡報 P5 內容

計畫合作期程

- 07~08 月 | 行政流程梳理、校內資料串接
- 09~10 月 | 發證系統安裝、系統整合測試
- 11~12 月 | 數位證書試發、各式問題處理

系統規格問題

- 數位證書系統主機建議規格為：CPU 2核心、RAM 2GB、儲存空間 100GB 以上
- 其餘規格問題，請參考「數位證書合作學校標準流程」

Q & A

如有不清楚的地方，歡迎各校聯繫詢問

教育部大專院校數位證書建置試辦計畫

計畫主持人：成功大學莊坤達副教授 / 舒宇宸副教授

計畫負責人：呂紹民 / smlu@netdb.csie.ncku.edu.tw

各類學位名稱訂定程序授予要件及代替碩士博士論文認定準則

- ① 學位證書內容應包括學生姓名、出生年月日、院、所、系、科、學位學程、組、畢業年月、學位名稱及證書字號
- ② 修讀本校或他校輔系或雙主修者，應另加註學校及學系名稱
- ③ 申請補發證明書者，並應包括補發證明書日期。

HashChain (雜湊鏈)

- 以 metadata 型式存在 PDF 檔案裡，僅用於判斷兩份 證書之間是否存在先後歷程關係
- 初發證書: $h_0 = \text{SHA256}(\text{seed})$
seed : 學號 + 身分證號 + salt字串 (儲存於各校 DB 中)
- 補發第 1 版:
 $h_1 = \text{SHA256}(h_0) = \text{SHA256}(\text{SHA256}(\text{seed}))$
- 補發第 2 版: $h_2 = \text{SHA256}(h_1)$
- 補發第 n 版: $h_n = \text{SHA256}(h_{n-1})$

Metadata List (中介資料列表)

- Hash : HashChain h_n value
- DDRelease : “v2” – framework version
- DDLanguage : “Chinese” or “English” – diploma language
- DDContent : $\text{AES_ENC}_{K_S}(\text{學號_學校ID})$ – index for hash in MOE DB

SHA256 (安全雜湊散列演算法)

- 用於計算 PDF 檔案的 checksum (數位指紋)
- 用於產生 HashChain 的 hash value

AES (進階加密標準、Rijndael 加密法)

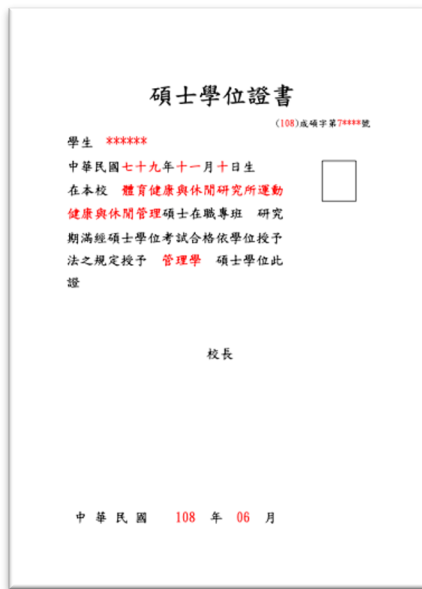
- 用於將資料庫的 index 加密，避免外流疑慮

SCP (安全傳輸協定)

- 用於將資料從各校發證主機上傳至教育部
- 上傳端 (各校) 用私鑰加密，接收端 (教育部) 用公鑰解密

PDF生成：畢業證書模板製作

各合作學校數位證書轉換作業流程



畢業證書模板製作

各校生成證書 PDF，並加入符合檢驗規定之資料

行政流程：整理數位證書樣式

各校因業務繁雜，衍伸出多樣畢業證書，版型可能因此未統一、規則化

建議：確認並整理校內證書樣式種類

系統串接：數位證書 PDF 生成

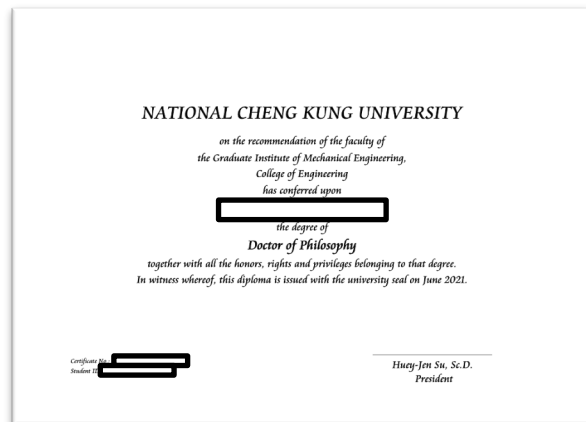
若各校原畢業證書無數位留存，尚無完整 PDF 生成機制可供使用，建議方法如下：

建議：

- (1) 匯出畢業列印系統產出之白底黑字文字
- (2) 準備好數位證書的底圖&校長簽章
- (3) 使用本計畫提供之工具將(1)與(2)進行合成

PDF生成：畢業證書模板製作

成大英文數位證書建置範例



數位英文證書範例

一般寄發：領取實體證書，由註冊組個別發證



批次寄發：學生申請後，由註冊組統一發證

(各校自行依據需求開發，團隊將提供發證 WEB API 供串接使用)
(僅適用於初次發證使用，須確保發證資料皆無誤)



全國大專院校數位證書試辦計畫

國立成功大學建置範例



領取時間: 110年6月24日至110年9月3日 上班時間
Dates Scheduled: During office hours from June 24 to September 3, 2021
領取地點: 教務處註冊組
Office: Registrar Division, Office of Academic Affairs
領取流程須知 The Note of Procedures for Receipt of Degree Certificates
[中文版](#) [English](#)
☒ 我已閱讀並清楚上述內容 I have read and agree

請確認個資正確，若有錯誤請洽註冊組修正
Please confirm that your personal data is correct, if there is any error, please contact Registrar Division for correction

學號 StudentID:	15404
姓名 Name:	陳榮 ZHI HEN
生日 Birthday:	09 1995
郵件信箱 email:	ba a@gmail.com is 2@gs.ncku.edu.tw
畢業學系:	醫學院 醫學系學士班 醫學學士
Dept./Inst. Degree:	Medicine Medicine Doctor of Medicine
☒ 確定申請畢業證書紙本郵寄，以下地址請填寫正確 Apply for Graduation (to receive your diploma) by mail, please fill in the following address correctly	
郵寄地址 Address:	221新北市汐止區忠三街

送出(submit) 離開(reset)

成大畢業離校系統確認畫面

確認姓名、生日、畢業科系、寄件 Email 是否有誤

註：Email 用於寄送數位學位證書、
地址用於寄送紙本學位證書（本年度因應疫情規劃）

國立成功大學
畢業生離校手續存查單 本地生(大學部)

注意：此單應由學生持送各單位蓋章後再繳教務處註冊組存查未辦清此單手續者不發給學位證書	二	一	辦理次序	學系：醫學系 班級： 學號：15404 姓名：陳榮 證書號碼：0109 2 40 104 1、因畢業離校所有借用圖書儀器及其他一切財物等歸還手續均清 2、在印出“本單”後，再去圖書館借書，未還清圖書前，不發給學位證書。 列印日期：1100609.0 列印時間：15:57:04
	辦成註冊 人續冊 承組	系 所	單 位	
			簽 章	
	申請郵寄證書	本加自個項各 組蓋定章手學 憑系最由續系 辦載後各及應 以務學蓋辦 庫籍至機何	備 註	

下載畢業離校手續存查單

將畢業離校存查單寄給系所蓋章，即完成申請程序



申請完成後，數位證書兩個工作日內將Email至：

(成大這邊亦正在著手規劃校內系統，以方便寄信後學生亦可以至註冊組指定位置下載)



個人信箱 (EX : kevinlu123@gmail.com)



成大永久學號 **gs** 信箱 (EX : H22301325@gs.ncku.edu.tw)