

# 公開金鑰加密系統於考試業務之應用

劉建康 連秋華

大學入學考試中心

## 摘要

本文主要針對大學入學考試中心應用公開金鑰加密系統在考試業務工作流程中的實際情況，從執行面的角度彙整說明。包括：(一)公開金鑰加密系統概述。(二)在考試業務的應用說明；包含題庫系統、試務軟體系統的備援、報名資料、選擇題 OMR 判讀結果、非選擇題紙面閱卷准考證條碼登錄及成績登錄、電腦螢幕閱卷、成績計算結果複核及成績通知等作業應用公開金鑰加密系統的過程逐一作說明。另對於包括制訂題庫 IC 晶片卡的卡片暨金鑰對管理辦法、集體報名單位報名系統暨成績查詢簡易應用公開金鑰加密系統之功能研發以及大學入學考試中心 PKI ( Public Key Infrastructure ) 公鑰建設基礎的應用及推廣等，提出相關建議事項。

**關鍵詞：**公開金鑰加密、非對稱式金鑰加密、數位簽章

---

劉建康，大學入學考試中心高級專員  
連秋華，大學入學考試中心專門委員