編號：（此欄位由主辦單位填寫）

中文專題名稱：SPIFFE 校園身分驗證系統

英文專題名稱：SPIFFE-based Campus Identity System

1. 前言

隨著校園資訊化的快速發展，學生與教師需要頻繁地存取各式各樣的系統與資源，例如課程平台、圖書館系統、研究資料庫與跨校合作平台。然而，傳統帳號密碼驗證方式不僅管理繁瑣，也存在安全性不足的問題，例如密碼外洩、重複使用、或權限難以及時調整。

近年來，國際間逐漸重視「零信任架構（Zero Trust Architecture）」與「統一身份管理」的需求，其中 SPIFFE（Secure Production Identity Framework For Everyone） 提供了一套標準化的解決方案，能以動態、安全的方式進行身份驗證與授權。

本系統的開發動機，即是將 SPIFFE 架構導入校園網路，使每一位師生、服務與設備都能擁有唯一且可信的身份標識，並透過自z動化憑證更新與授權管理，提升校園網路的安全性與便利性。我們希望藉此實現一個兼具 安全、彈性與前瞻性 的智慧校園身份驗證模式，為未來的校園資訊環境奠定更穩固的基礎。

1. 創意描述

本系統的創意核心在於將 SPIFFE（Secure Production Identity Framework For Everyone）標準 引入校園網路環境，藉由統一且動態的身份管理機制，解決傳統校園網路中身份驗證與授權分散、難以擴展的問題。

在現行的校園網路架構中，師生常透過學號、帳號密碼或臨時憑證進行驗證，但這些方法存在安全性不足與管理成本高的問題。若結合 SPIFFE，我們可以為每一個使用者、應用服務與網路資源分配安全的 SPIFFE ID，並透過 SVID（SPIFFE Verifiable Identity Document） 自動完成身份驗證與憑證更新，達到去中心化、零密碼化的安全身份信任模式。

**本系統的創新點在於：**

1.身份即服務：將校園內所有網路節點（伺服器、應用程式、IoT 裝置）都能以 SPIFFE ID 被識別。

2.動態信任架構：學生、老師可在不同課程、研究專案或跨校資源共享時，自動獲取相應的授權，不需再依賴繁瑣的人工帳號建立或權限設定。

3.比賽應用場景：藉由校園網路結合 SPIFFE，可以模擬大規模分散式系統的安全管理，展現校園資訊系統如何以業界前瞻的標準強化安全性，並兼顧靈活性與擴展性。

此創意結合「校園情境」與「國際標準」的特色，不僅能增強學z校網路的安全性，還能作為未來智慧校園的示範案例，具備創新性與實用價值。

1. 系統功能簡介

* 身份驗證功能

透過 SPIFFE ID 與 SVID，自動為學生、教師、伺服器及校園設備進行安全身份驗證，取代傳統帳號密碼登入方式。

* 授權與存取控制

系統依照課程、專案或角色，自動分配相對應的資源使用權限，並能隨使用情境動態調整。

* 資源與服務整合

提供統一的身份信任平台，支援校園常用服務（如課程平台、圖書館系統、研究資料庫）及 IoT 裝置的存取。

* 自動憑證管理

SVID 憑證由系統自動生成、更新與撤銷，降低管理者的人力負擔與錯誤風險。

* 跨網域支援

允許跨校合作或不同網路環境下的安全身份互認，支援分散式與雲端資源存取。

* 管理與監控介面

提供管理員操作介面，用於檢視使用者身份狀態、授權紀錄與資源存取情形，確保系統透明與可控。

1. 系統特色

* **零密碼化驗證**

不再依賴傳統帳號密碼登入，透過 SVID 憑證 即可完成自動化身份驗證，降低帳號被盜用或密碼洩漏的風險。

* **統一身份管理**

以 SPIFFE ID 為核心，所有使用者（師生）、應用服務與設備皆能被唯一識別，避免傳統帳號系統分散管理的困境。

* **動態授權機制**

學生或教師在不同課程、研究專案中，可即時獲得對應的存取權限，授權可隨情境變化而自動調整，無須人工干預。

* **跨平台與跨網域支援**

無論是校園伺服器、雲端資源或 IoT 裝置，皆可透過 SPIFFE 架構進行身份信任，達成跨平台的安全互通。

* **提升校園資訊安全標準**

系統採用國際通用的 SPIFFE 標準，使校園網路安全性與業界接軌，能有效抵禦憑證竊取、內部濫用等常見攻擊。

* **智慧校園應用前瞻性**

此系統不僅可應用於課程管理、圖書館系統、研究合作，也能延伸至智慧校園 IoT 裝置，展現未來校園全面數位化的可能性。

1. 系統開發工具與技術
2. **身份與安全框架**

* SPIFFE (Secure Production Identity Framework For Everyone)：提供統一的身份標準與信任模型。
* SPIRE (SPIFFE Runtime Environment)：用於在實際環境中發放與驗證 SPIFFE ID 及 SVID 憑證。

1. **程式語言與後端框架**

* Go / Python / Java：用於撰寫伺服器端 API 與身份管理邏輯。
* Node.js / Express：支援校園應用服務的後端建置。

1. **前端技術**

* React / Vue.js：開發使用者介面，方便學生與老師操作。
* HTML5 / CSS3 / JavaScript：基礎前端技術，確保跨平台相容性。

1. **資料庫系統**

* PostgreSQL / MySQL：儲存使用者、課程、授權紀錄等資料。
* Redis：作為快取與 Session 管理，提高系統效能。

1. **容器與部署環境**

* **Docker**：將各服務容器化，方便模擬不同校園網路節點。
* **Kubernetes (K8s)**：進行容器編排，模擬大規模校園環境下的服務自動化部署與擴展。

1. **網路與系統管理工具**

* **Linux (Ubuntu / CentOS)**：伺服器環境。
* **Nginx**：反向代理與負載平衡，確保系統穩定性。
* **OpenSSL**：搭配 SPIFFE，驗證與測試憑證功能。

1. 系統使用對象

* **學生：**登入課程平台、圖書館系統、研究資料庫。
* **教師：**課程管理、研究專案協作、跨校資源共享。
* **系統管理員：**進行身份驗證管理、授權設定與監控。

1. 系統使用環境

* **伺服器端：**Linux (Ubuntu/CentOS) + Docker/Kubernetes 部署。
* **前端端：**支援 Chrome / Safari / Edge 等常見瀏覽器。
* **校園網路環境：**有線/無線網路，支援跨網域協作。

八、結語  
 本系統將 SPIFFE 標準 引入校園網路環境，成功解決傳統帳號密碼機制在管理與安全上的限制，並建立起一個統一、可信且動態的身份驗證與授權平台。透過零密碼化驗證、自動化憑證管理與跨平台支援，系統不僅能強化校園資訊安全，亦能有效提升使用者體驗與資源利用效率。

此創新設計展現了 智慧校園 與 前瞻網路安全技術 的結合潛力，未來更可延伸應用至跨校合作、研究資源共享及 IoT 校園裝置，成為打造安全且靈活的數位校園典範。我們期望此系統能在比賽中展現出「安全、創新、可持續發展」的價值，並作為未來智慧校園的重要參考架構。