

# 認證雲 - 成績登錄應用系統

## Authentication Cloud, Applied To Student Score Uploading System

指導教授：黃宗立

專題成員：胡家瑋

開發工具：HTML5、Java、PHP

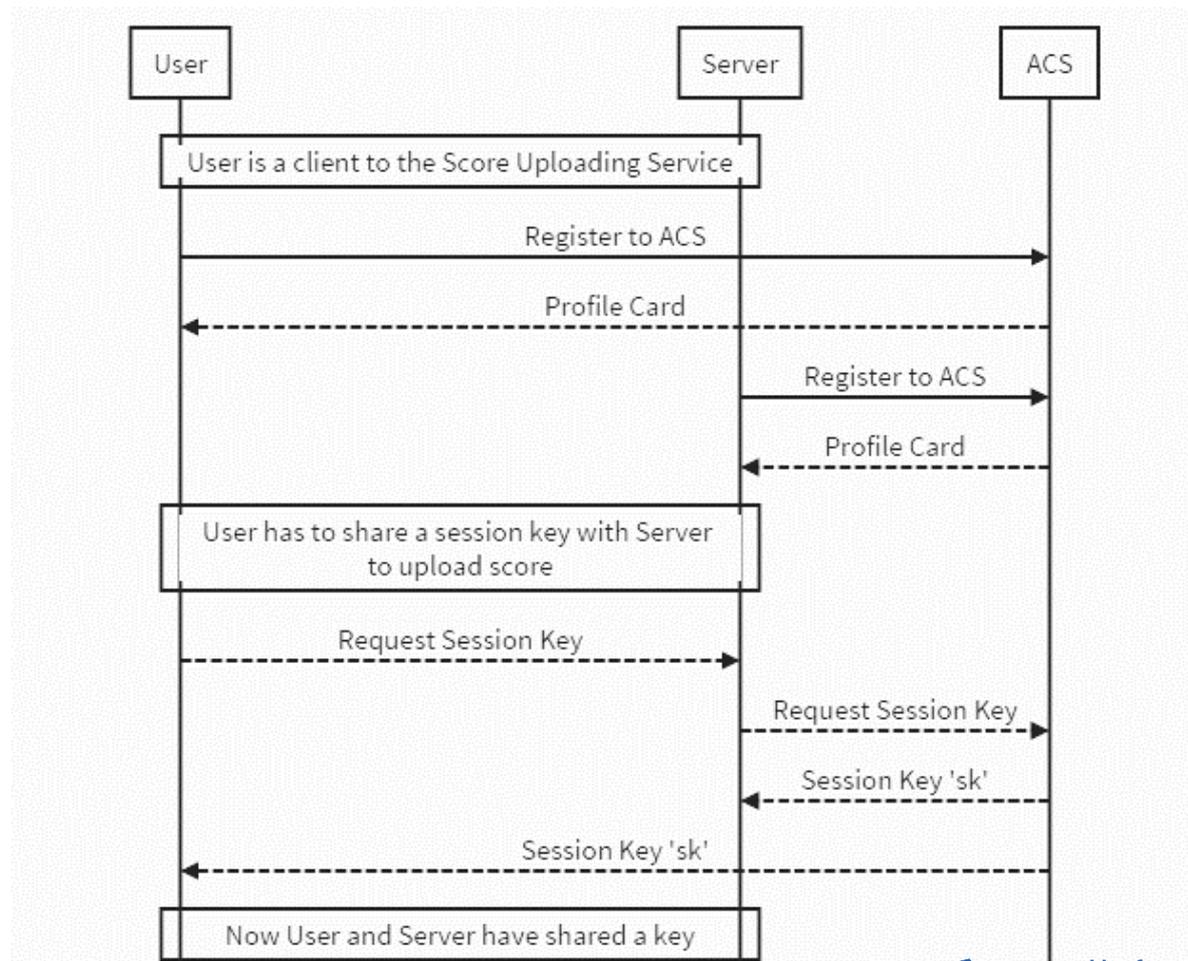
測試環境：Chrome、Firefox、JDK8、Apache2

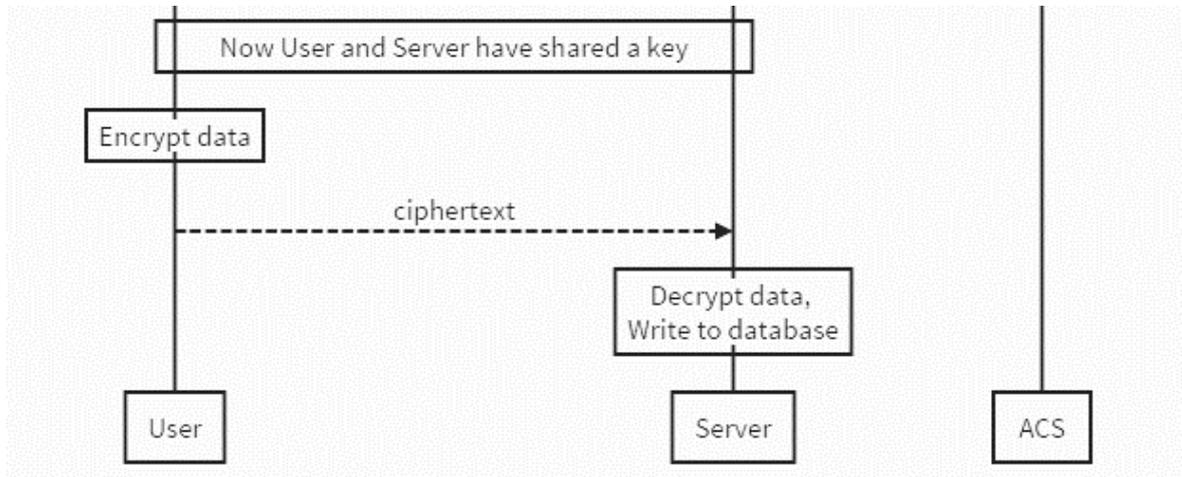
### 一、簡介

現今許多網路加密傳輸過程乃是基於公鑰協定，但由於量子電腦發展日新月異，許多常用的公鑰系統將可能被破解，通訊的雙方如何約定金鑰便成為一大難題。因此我們使用雲端認證伺服器 (ACS) 實作出一套基於雜湊法的金鑰分配系統，以此為網路伺服器與其使用者之間分配一把通訊用的金鑰。

本專題以學生成績登錄系統為例，展示認證雲在成績登錄伺服器與成績登錄者（教師）之間分配金鑰的結果。使用者能以此金鑰加密上傳的成績，將密文上傳至伺服器之後再由成績登錄伺服器解密。

系統架構圖：





## 二、 測試結果

成功完成金鑰分配：

Choose profile :  profile\_registered (4).card or Enter your ID in this computer :

Profile password :

Profile ID: 3ddd472525986932f2d737cda2e88c36d6010b827cb0b0f02e1afa14c1886e8d

SessionKey: 0e89babe3a92aca82c06882c164ba6f735b514b01a7845377a58b7a40ee14c61

[Download new profile](#)

使用此通訊金鑰加密之後的密文：

localhost 的網頁顯示:

本資料已使用認證式加密保護

成大資工系  
量子資訊安全實驗室

---

Example 1: Manual Input and Encrypt

學號	姓名	
<input type="text" value="F74012345"/>	<input type="text" value="王小明"/>	<input type="text" value="100"/>
<input type="text" value="F74013579"/>	<input type="text" value="李小美"/>	<input type="text" value="99"/>
<input type="text" value="F74024689"/>	<input type="text" value="林小華"/>	<input type="text" value="98"/>

KEY= a0e993753540c0c0a56d17e8568a640a  
IV= c7f3a80c41f70e4fafcbbc931130760bf

密文=