## Case Study 3: Implementing PKI on smart devices for Education – Universities.

**Background:** There are many Universities that have started deploying policies and infrastructures to support electronic authentication of entities (staffs, professors/lecturers/tutors, students, etc). One main application of this is to digital sign electronic documents.

**The scenario:** The university issues official transcripts in electronic PDF format, using PDF signing technology. Consider expanding this model on educational areas, to enable the entities to exchange documents electronically and to achieve a complete paperless environment using a PKI model with smart devices. All the students are now required to submit their assignments and course works to their lecturers/tutors electronically via their tablets.

**Assumption:** Each student will be issued a valid digital certificate and a tablet by the university. On the other hand, the lecturers/tutors will send the marks/score to the student electronically too. The scope can further cover to online test and exam with the assumption the university have their e-learning system ready.

**Basic Requirements**

- Mobile assignment submission
- Online test or exam participation
- Mobile authentication and authorization
- Assignment marking or score reporting

**Technology to use:**

Client side signature services

- PKI Smart card (option with mobile reader)
- PKI Micro SD Card (option with mobile reader)
- SIM-based PKI
- Software-based PKI

Server based signing services

- Sign Server using HSM
- Verification Server

Authentication mechanisms

- Encrypted SMS
- QR codes
- One Time Password Generator
- PIN codes

Management Systems

- Certificate Management
- Card, and Key, Management System

**Questions**

1. Which particular technology or combination of technologies would best fit for this project?
2. Explain your justification of the chosen solution.
3. List down other facts which are crucial to evaluate the proposed solution.
4. List down possible challenges to implement the proposed solution.
5. How to hide PKI complexity from the users?