Case Study 2:
Implementing PKI on smart devices for eFilling.

Background: Every year, taxpayers in most countries are required to declare their annual income to their local Tax Authority. Traditional ways to file income tax include: (a) in-person, (b) in-person by representative, (c) by mail, (d) in-person by authorized third-party entity (e.g. tax agency or commercial bank) etc. All of the methods involve a lot of paperworks and red tape by Tax Authority. Thus, many countries started promoting online tax filing.

The scenario: The citizens are now able to perform their e-filling via the Tax Authority portal, they will be able to input with real time automated tax calculation. The citizens will need to digitally sign for their final submission. The citizens can obtain their digital certificates from any of the licensed public certificate authorities. In order to be able to perform online tax filing, they must first obtain an online tax filing ID from the Tax Authority.
Consider an expanded PKI model where the above scheme would be changed to support submission of income tax returns using a mobile application on a smart device.
Special requirement: to be authenticated/authorized ONLY by your digital certificate without the need of username, password or any IDs.

Basic Requirements

- Mobile authentication
- Form filing and submission
- Fallback authentication method

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?