Case Study 1: Implementing PKI on smart devices for banking services.

Background: Many people nowadays rely on e-banking for their businesses and personal lives. As banks always strive to improve and expand the accessibility of their services while aiming to reduce their operational costs, e-banking and m-banking have become more popular. Most e-banking and m-banking solutions are basically web applications where input data are protected using SSL for communications and transactions are protected/authorized by use of client based digital certificates and/or dynamic password system.

The scenario: You are assigned to design/implement an m-banking application (thin-client) which aims to offer traditional e-banking services by using secure WEB service. Data between application and bank servers are exchanged using a simple XML protocol. XML data sent will be encrypted and digitally signed by corresponding party using a PKI model. The application should be user-friendly, capable to support variety of m-banking services, easier to adopt and expandable to new requirements.

Basic Requirements

- Login authentication via smart devices
- Transaction authorization
- Electronic statement
- XML data validation

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?