Case Study 5: Implementing PKI on smart devices for a multinational company.

Background: There are upcoming trends of green initiative where more companies are implementing paperless working environment via electronic document management system. PKI has been widely used for this implementation that also supports digital signature, in line with their organization approval workflows.

The scenario: A multinational company with international branches wants to migrate their users from PC based to tablet based. The company already has PKI and electronic document management system in place. You are now assigned to lead the migration project and must propose the best method to retain their existing PKI workflows.

Basic Requirements

- Mobile authentication
- PDF Signing/Validation
- File Encryption
- S/MIME support

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?