Case Study 4: Implementing PKI on smart devices for Healthcare services.

Background: Healthcare services are the topmost importance for citizens all around the world. However, most governments face serious challenges to manage patient medical records that consist of highly P&C information while implementing the e-Health system.

The scenario: A country has successfully implemented a nationwide e-Health system where all patient records are safely kept in a centralized database, which integrates with all hospitals and clinics. Any authorized users (staffs, doctors, pharmacist, etc.) must perform PKI authentication and authorization before able to access, submit or update any patient medical records.

As demanded by the citizens, before anyone is allowed to access their medical records, the system must get their approval by applying PKI model via smart devices.

Exceptional condition: emergency cases where doctor can override it without the approval.
Assumption: when the first medical record being created, a digital certificate is already issued to the citizens.

You are now assigned to extend the existing e-Health system to cover patient approval via smart devices as per the above scenario.

Basic Requirements
- Mobile authentication
- Mobile approval with authorization
- Must achieve Non-repudiation

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?