

1. Which particular technology or combination of technologies would best fit for this project?

Banking	Hybrid solution – Mobile app with Login/Password combination for simple authentication and low amount transfers SIM-based for large amount transfers
Government	Company -Mobile-PKI smartcard with reader, Individual-Server signing services with OTP
Education	Software based PKI combined with SMS
Healthcare	OTP via SMS & PIN from patients mobile phone, Doctor has a device with smartcard reader + fingerprints. Central Database for private keys
Multinational companies	Sign and encryption server with HSM + hardware OTP in a HTTPS environment.

2. Explain your justification of the chosen solution.

Banking	High market coverage, keep high level of security for crucial operations, ease of use, ease of distribution
Government	Company- High degree to security, Individual-Lower cost compare to smartcard PKI
Education	Only cost effective enough, easier distribution
Healthcare	To provide access to patients file in emergency – server signing. Simplicity for the patients
Multinational companies	Not necessary to have a regulation to use client signing as long as achieving objective.

3. List down other facts which are crucial to evaluate the proposed solution.

Banking	Legislation, Mobile device usage amongst the population, solution's lifetime
Government	Compliance to country CP & CPS, On the go mobility capability
Education	Controlled environment, easier to manage
Healthcare	Distribution to doctors for mobile terminals to access medical files. Time stamp solution in case doctors key is compromised
Multinational companies	Functionality vs cost. Cost effective solution must be chosen

4. List down possible challenges to implement the proposed solution.

Banking	Distribution, GSM operator dependence, Legislation
Government	Key & cards management cycle, end user adaptability to mobile PKI services, no common standard between different devices
Education	Students change mobile numbers often. Need for re enrollment.
Healthcare	Availability of patients phone, user friendliness, difficulty to collect all data in a single database.
Multinational companies	File size limitation and processing power limitation in mobile. Integration with mobile signing application

5. How to hide PKI complexity from the users?

Banking	Provide easy to learn and easy to adapt user interfaces, use minimal hardware possible
Government	Simplify cert and card management process. Ex transparent auto certificate management. Auto enrollment & renewal process
Education	The user does not know he is using PKI. Enrollment is used with a simple QR code.
Healthcare	PKI is invisible to the patient he only writes down his pin and OTP via SMS or Token
Multinational companies	User provides OTP and password with PKI transparent to them