FIGI Security Clinic

App Security Framework

Rehan Masood
State Bank of Pakistan

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Country Landscape

- High cell-phone penetration
  - Mobile density stands at 77%; more than 162 million NADRA* verified cell phone connections
- High internet usage
  - More than 71 million mobile 3G/4G/LTE users
- 60% population under the age of 45 years
- Adopted National Financial Inclusion Strategy in 2015
- National Payment System Strategy in Nov 2019

DFS Potential**

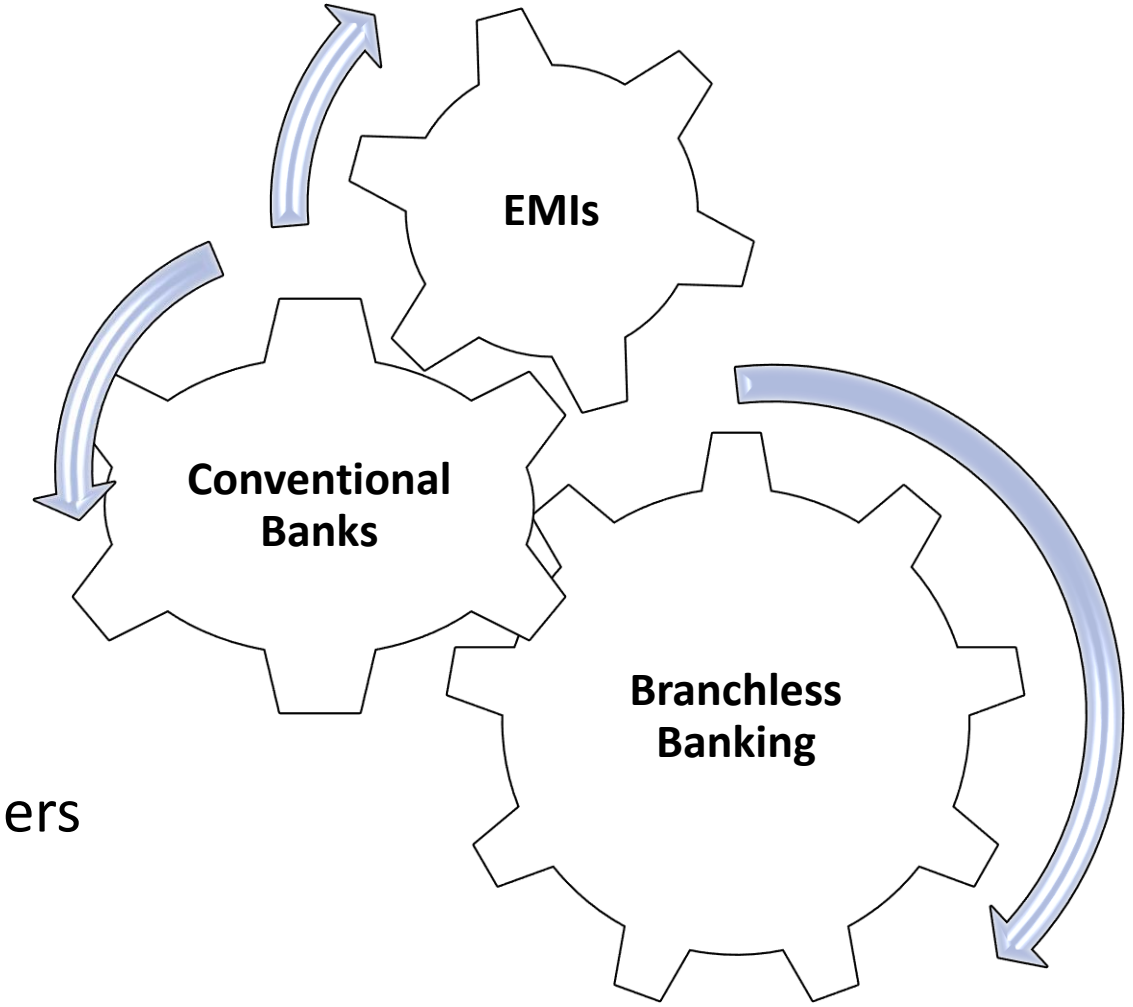
- 7% boost to GDP by 2025
- 4 million new jobs
- US$ 263 Billion new deposits

*National Database & Registration Authority

**MCKINSEY GLOBAL REPORT, "DIGITAL FINANCE FOR ALL: POWERING INCLUSIVE GROWTH IN EMERGING ECONOMIES" SEP 16

DFS Market

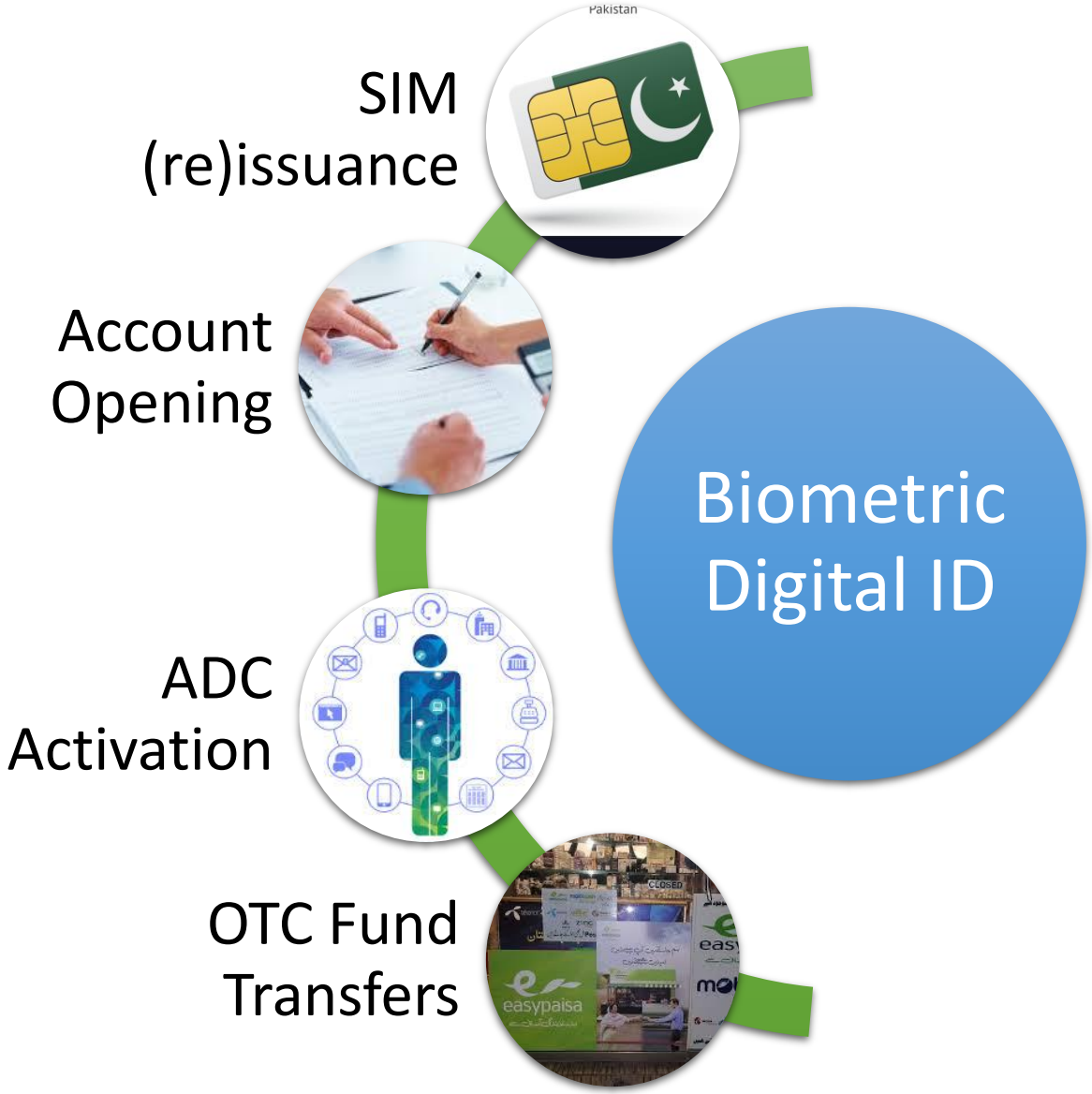
- **Branchless Banking**
  - 11 licensed providers
  - 38 million BB accounts
  - 420,000 BB Agents
  - 21 million USSD users; 7 million app users
- **Conventional Banking**
  - 23 Bank Apps
  - 6 million users
- **EMIs**
  - Regulations aimed at removing entry barriers for non-banking companies
  - Issue e-money for payment services



DFS Stakeholders

- Users
- Mobile Network Operators (MNOs)
- DFS Providers
- Retail Agents
- Banking Regulators
- Telecom Regulators
- Identity Verification Services
- Third Party Service Providers

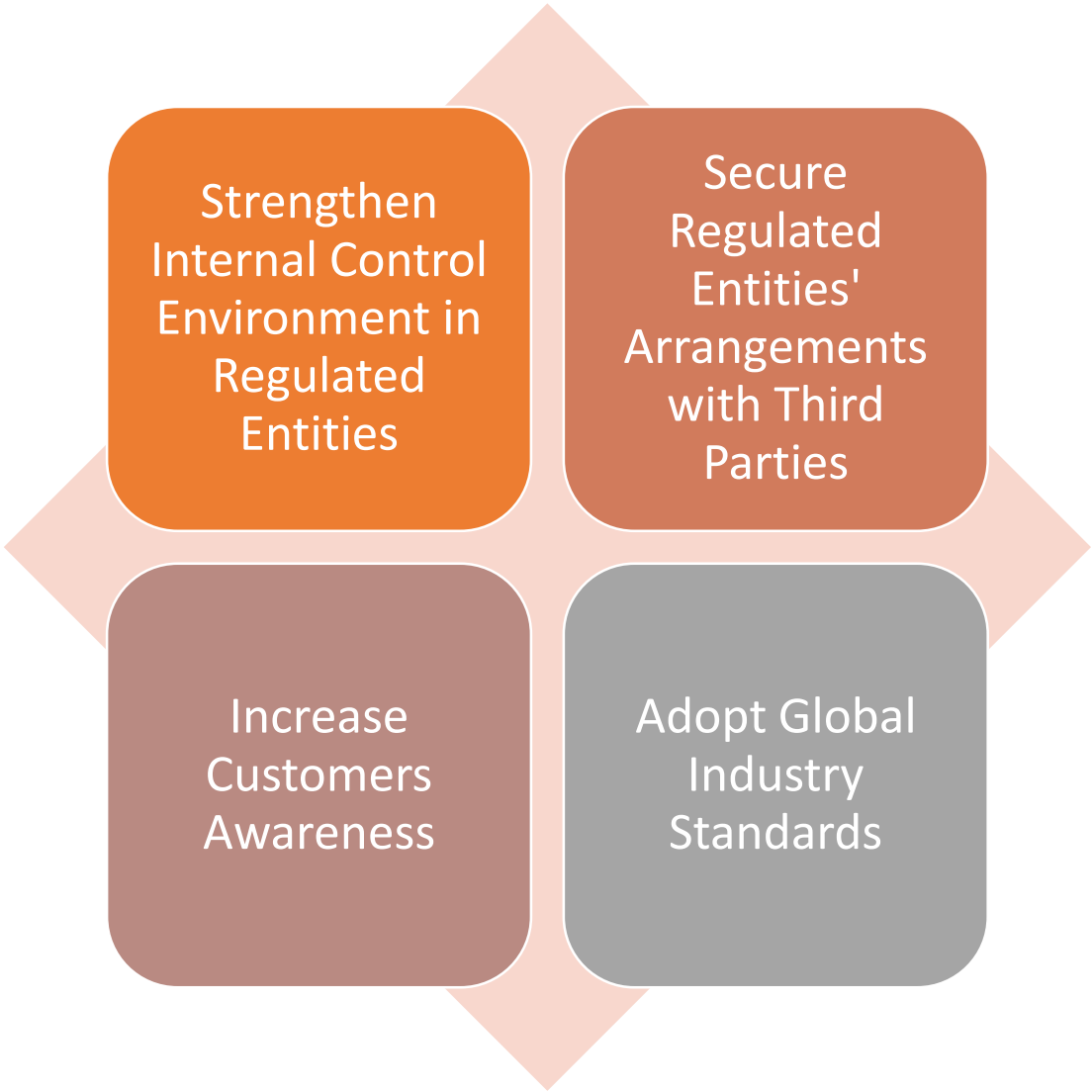
Digital ID stack



App Security Framework Scope

- Applicable to all banks, branchless banking providers, EMIs, PSPs
- Addresses mobile applications for smart devices
- Covers mobile app ecosystem processes involved in:
  - capturing, storing, processing and transmitting financial/non-financial information
- Includes people, processes, infrastructure including:
  - mobile apps, web services, server-side databases, storage and network communications etc.

Intended Outcomes

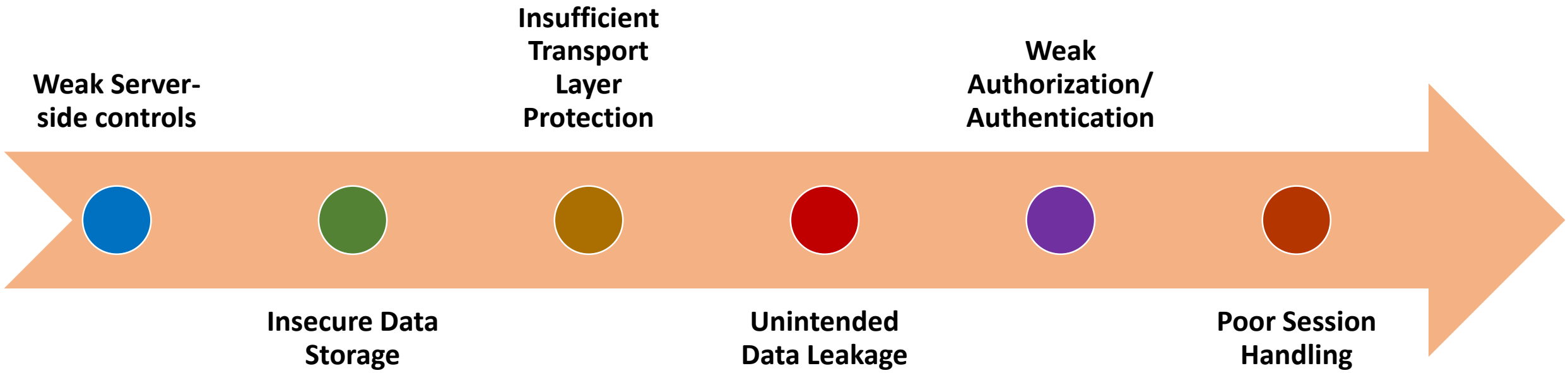


Applicability

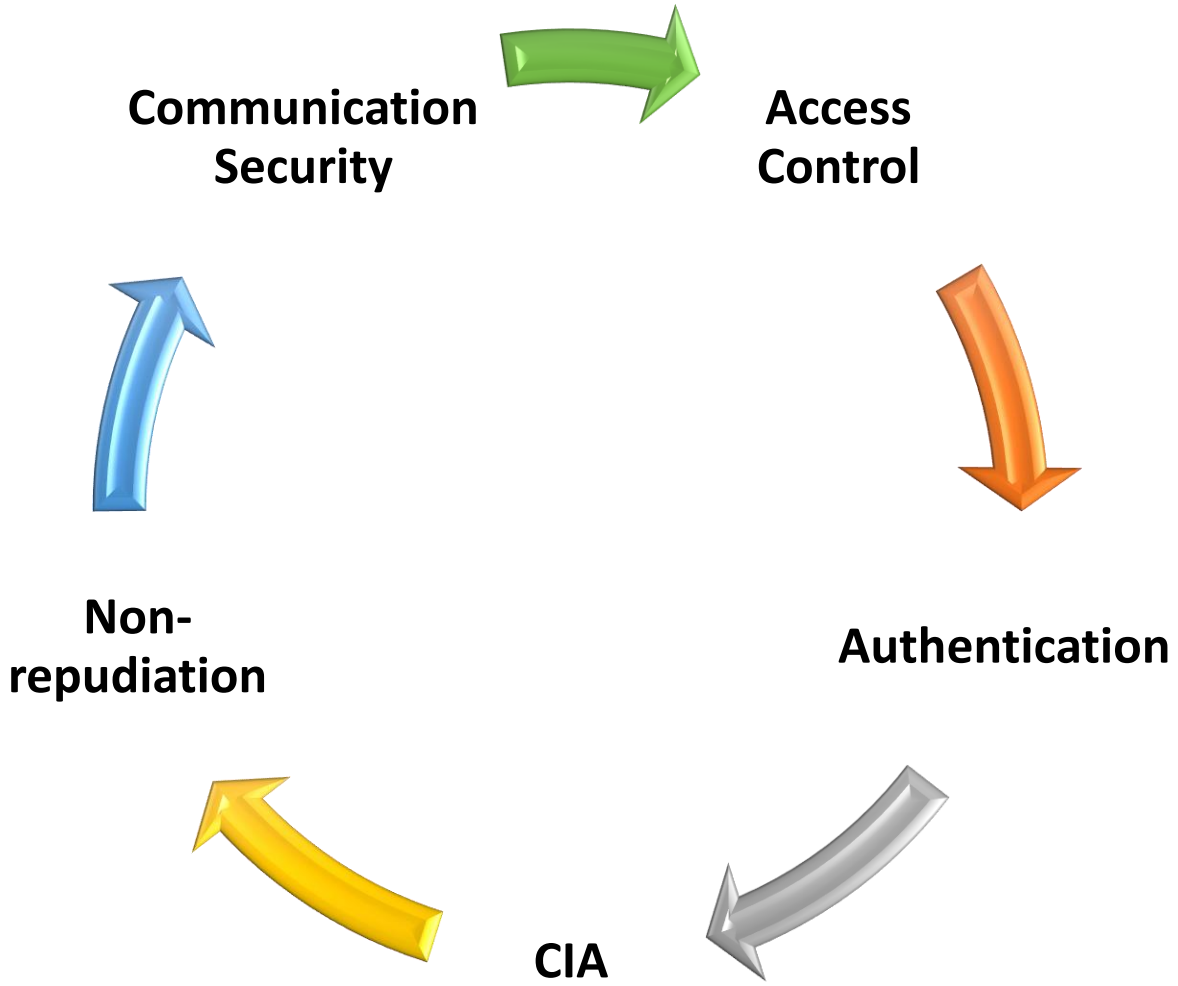
- App owners shall use this framework for:
  - Architecture
  - Design
  - Development and
  - Deployment

- App owners shall ensure that the requirements in this framework are used by architects, developers, testers, security professionals, and consumers to define and understand the qualities of a secure mobile app.

Major Vulnerabilities



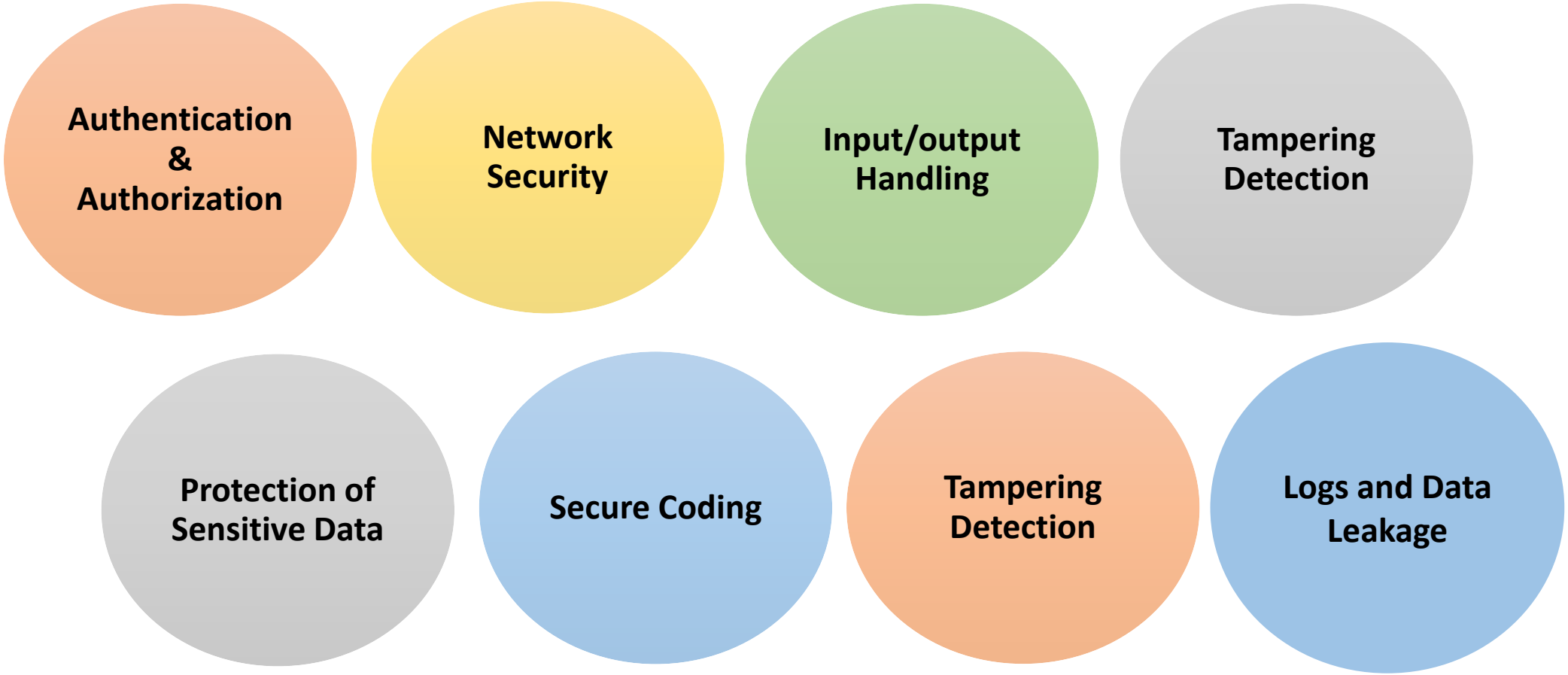
Security Dimensions



References

- International Telecommunication Union (ITU)
  - ITU-T Focus Group Digital Financial Services: Security Aspects of Digital Financial Services (DFS)
  - X.805 : Security architecture for systems providing end-to-end communications
- OWASP Mobile Application Security Project
- National Information Assurance Partnership
  - Protection Profile for Application Software

Mobile App Security Requirements

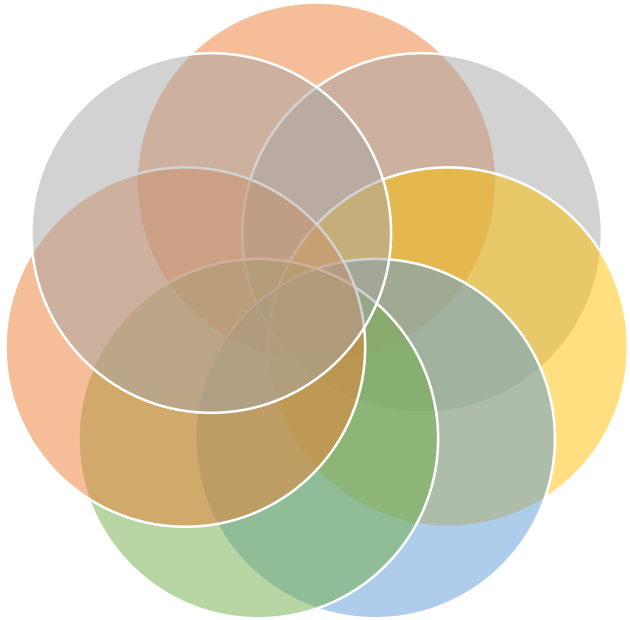


Authentication and Authorization

Device binding and account tagging

Idle session termination

Biometric-based activation



Strict minimum validity of OTPs

Separate login authentication and transaction authorization

Strong, configurable access codes (PIN/Password, bio)

Multifactor authentication

Protection of Sensitive Data

- PCI-DSS
- Sensitive information not to be stored on mobile devices
- Use of industry standard cryptography
- Encryption of sensitive data in-transit and at rest
- Sensitive data shall not be transmitted through vulnerable channels

Network Security

- Transport layer encryption for all communications between the mobile app and servers.
- Inbuilt controls to mitigate bypassing of certificate pinning
- Certification errors shall not be ignored
- Use of valid certificates issued by a trusted certificate authority

Session Management

- Automatic user-logoff functionality after a configurable idle time-period
- Easy to use and clearly visible logoff method
- Disable access to mobile app server from devices which are reported lost or stolen.
- Procedure for customers to report lost or stolen devices
- Detect multiple simultaneous login attempts and communicate it to the users

Tampering Detection

Checks on server-side to verify mobile app integrity and to detect any manipulation.

Installation of mobile apps not allowed on rooted/jail broken devices.

Debugger/emulator detections in place

Secure Coding

Adhere to industry accepted secure coding practices and standards

Avoid vulnerable/deprecated components, protocols, libraries, scripts etc

Code signing shall be used for mobile apps

Input and Output Handling

Data to be sanitized and validated

Auto-complete feature shall be disabled for sensitive information

Clipboard/ copy-paste function shall be disabled for sensitive data

Logs and Data Leakage

- Mobile app logs shall not contain any sensitive data
- Log server shall be segregated from application servers
- Protect the logs from unauthorized modification or destruction
- Audit logs shall be maintained at the server level
- Retain logs for a period of 05 years at a minimum

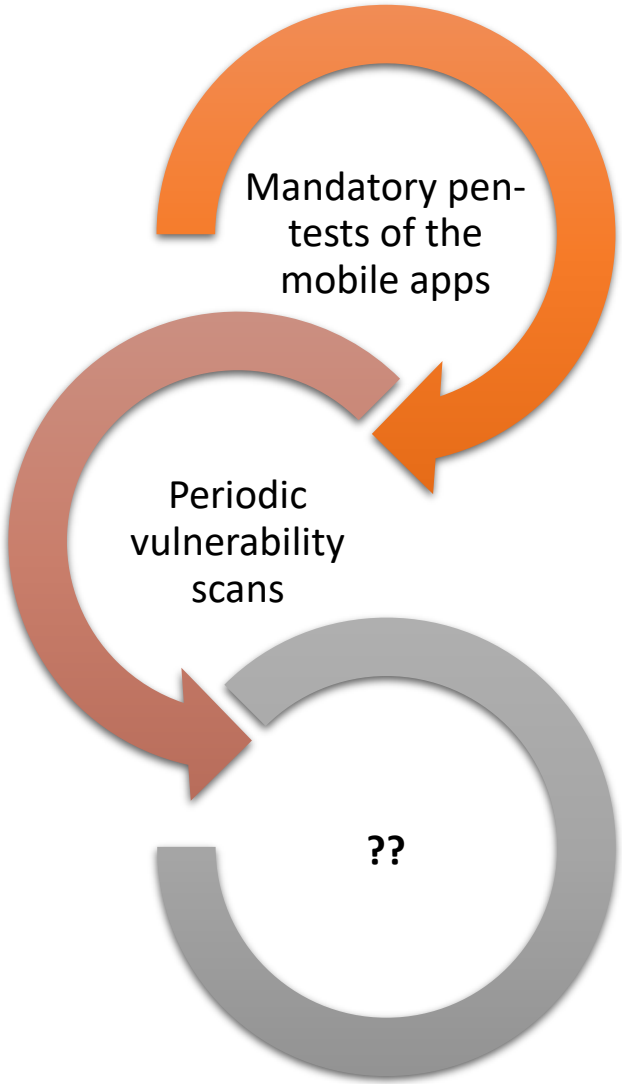
App Hosting

Mobile apps shall be hosted only at the relevant platform store such as Google Play Store, App Store

Shall not be hosted at app owner’s website or the vendor website or any other third-party website

Ensure that all users are informed that its mobile app is not hosted on third party stores

How to assess compliance?



Thank you