ภาคผนวก ซ

การพัฒนา Mobile Application

คุณสมบัติเฉพาะของการพัฒนา Mobile Application

๑. การวิเคราะห์ความต้องการ (Requirement Analysis)

๑.๑. ผู้รับจ้างต้องเก็บความต้องการ (Requirement) โดยร่วมกับผู้ว่าจ้าง เพื่อจัดทำเอกสาร SRS (Software Requirement Specification) ครอบคลุม Functional, Non-Functional, Security, Performance, Compliance

๑.๒. ต้องมี Use Case, User Story, Acceptance Criteria ครบถ้วน

๑.๓. Requirement ต้องมีการ Traceability เชื่อมโยงไปยัง Test Case

๒. การออกแบบสถาปัตยกรรมและเทคโนโลยี (System Design & Architecture)

๒.๑. Mobile Application ต้องพัฒนาด้วย Cross-Platform Hybrid Framework ที่สามารถ Compile เป็น Native iOS และ Android จาก Single Codebase

๒.๒. Framework ที่ใช้ต้องรองรับ

๒.๒.๑. Hot Reload / Hot Restart เพื่อความรวดเร็วในการพัฒนาและทดสอบ

๒.๒.๒. Reactive Programming Model สำหรับการจัดการ State และ UI

๒.๒.๓. Ecosystem สำหรับ Security และ Performance Optimization เช่น Code Obfuscation, Secure Storage

๒.๓. การออกแบบซอร์สโค้ดต้องใช้หลักการ Clean Architecture / MVVM หรือเทียบเท่า เพื่อความเป็นระบบและง่ายต่อการบำรุงรักษา

๒.๔. Dependency Management

๒.๔.๑. ต้องใช้ Package Manager ที่มีการตรวจสอบช่องโหว่ (เช่น การทำ SCA พร้อมรายงาน SBOM รูปแบบ CycloneDX/SPDX)

๒.๔.๒. ห้ามใช้ Library ที่ไม่มีการอัพเดตเกิน ๑๒ เดือน หรือไม่มี Source Code ที่ตรวจสอบได้

๒.๕. Secure Build Pipeline:

๒.๕.๑. ใช้ CI/CD Pipeline ที่มีการ Scan ช่องโหว่ (SAST, DAST) และ Software Composition Analysis (SCA)

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

๒.๕.๒. ต้องมี Code Signing สำหรับ Application Package

๒.๖. Application ต้องสามารถเชื่อมต่อและทำงานร่วมกับระบบ Microservices ได้อย่างราบรื่น โดยสื่อสารผ่าน API Gateway (REST/gRPC/GraphQL) ตามที่ระบบกลางกำหนด

๒.๗. ต้องบูรณาการกับระบบกลาง เช่น Identity Provider, Logging, Monitoring

๓. มาตรฐานและ Best Practices ด้านความปลอดภัย (Security)

๓.๑. การพัฒนาระบบต้องเป็นไปตามหลัก Secure by Design และอ้างอิงมาตรฐานสากล ดังนี้

๓.๑.๑. OWASP Mobile Security Testing Guide (MSTG)

๓.๑.๒. OWASP MASVS (Mobile Application Security Verification Standard)

๓.๑.๓. OWASP Mobile Top 10

๓.๑.๔. NIST SP 800-163: Vetting the Security of Mobile Applications

๓.๑.๕. ISO/IEC 27001 และ ISO/IEC 27034 (Application Security)

๓.๒. การเข้ารหัสข้อมูล

๓.๒.๑. ข้อมูลผู้ใช้และข้อมูลสำคัญต้องเข้ารหัสด้วย AES-256 หรือสูงกว่า

๓.๒.๒. การสื่อสารทั้งหมดต้องผ่าน TLS 1.2 ขึ้นไป และต้องเปิดใช้ Certificate Pinning

๓.๒.๓. เปิดใช้ HSTS (HTTP Strict Transport Security)

๓.๒.๔. Certificate Pinning ต้องรองรับการ Rotate Certificate

๓.๒.๕. iOS ต้องเปิดใช้ App Transport Security (ATS), Android ต้องกำหนด Network Security Config สำหรับ pinning

๓.๓. Authentication & Authorization

๓.๓.๑. Session Timeout และ Token Expiration

๓.๓.๒. ใช้ PKCE (Proof Key for Code Exchange) สำหรับ OAuth 2.0 / OpenID Connect หรือ JWT

๓.๓.๓. รองรับ Multi-Factor Authentication (MFA)

๓.๓.๔. รองรับ Biometric Authentication (เช่น Fingerprint, FaceID)

๓.๔. Secure Coding

๓.๔.๑. ปฏิบัติตาม OWASP Secure Coding Practices

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

๓.๔.๒. ใช้ Obfuscation เพื่อป้องกัน Reverse Engineering

๓.๔.๓. ห้ามเก็บ API Key / Secret ไว้ในโค้ดหรือไฟล์ config แบบ Clear Text

๓.๔.๔. ใช้ Static Code Analysis (เช่น SonarQube) เป็นส่วนหนึ่งของ Quality Gate

๓.๔.๕. ห้ามใช้ Hardcoded Credentials

๓.๔.๖. เปิดใช้ ProGuard / R8 สำหรับ Android และ Bitcode สำหรับ iOS

๓.๕. Version Control & Branching Strategy

๓.๕.๑. ซอร์สโค้ดทั้งหมดต้องถูกจัดเก็บและบริหารจัดการบนระบบ Version Control (เช่น Git) ที่รองรับการกำหนดสิทธิ์เข้าถึง (Access Control) อย่างปลอดภัย

๓.๕.๒. การพัฒนาต้องดำเนินการตาม Git Flow หรือ Branching Model ที่องค์กรกำหนด (เช่น main/master, develop, feature, release, hotfix) เพื่อให้การทำงานเป็นระบบและง่ายต่อการตรวจสอบย้อนกลับ

๓.๕.๓. ต้องมีการบังคับใช้ Code Review (Pull Request/Merge Request) ก่อนรวมโค้ดเข้าสู่ main branch

๓.๕.๔. ต้องเปิดใช้ Protected Branch และ Commit Signing (GPG/SSH) เพื่อความมั่นใจในความถูกต้องและความปลอดภัยของซอร์สโค้ด

๓.๖. Reverse Engineering Protection

๓.๖.๑. ใช้ Obfuscation + Anti-Tampering + Root/Jailbreak Detection

๓.๖.๒. ตรวจสอบ Emulator และ Debugger Detection

๓.๗. Attestation/Integrity

๓.๗.๑. iOS ต้องรองรับ DeviceCheck/App Attest เพื่อยืนยันความถูกต้องของแอป/อุปกรณ์ก่อนให้เข้าถึงทรัพยากรสำคัญ

๓.๗.๒. Android ต้องรองรับ Play Integrity API ตรวจสอบสภาพแวดล้อม (device/app integrity) ก่อนอนุญาตการทำธุรกรรมสำคัญ

๔. การบูรณาการกับ DevSecOps, CI/CD และ Monitoring

๔.๑. Mobile Application ต้องพัฒนาภายใต้กระบวนการ DevSecOps โดยมีการ Shift-Left Security ตั้งแต่ระยะต้นของการพัฒนา

๔.๒. ต้องรองรับการผนวกรวมกับ CI/CD Pipeline ขององค์กร โดยอย่างน้อยต้องมี

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

๔.๒.๑. Static Code Analysis (SAST), Dependency Scanning (SCA), Dynamic Application Security Testing (DAST) เป็นขั้นตอนบังคับ (Quality/Security Gate) ก่อนเผยแพร่

๔.๒.๒. Automated Build & Deployment ไปยัง TestFlight (iOS) และ Firebase App Distribution / Google Play Internal (Android)

๔.๒.๓. รายงาน SBOM และรายงานช่องโหว่ต้องแนบเป็น artifacts ของ pipeline

๔.๓. ต้องสามารถ Integration กับระบบ Microservices ที่มีอยู่ โดยผ่าน API Gateway และต้องรองรับ Service Discovery ตามมาตรฐานระบบกลาง

๔.๔. ระบบต้องรองรับ Centralized Monitoring ครอบคลุมทุก Service ที่เกี่ยวข้อง เช่น

๔.๔.๑. Application Performance Monitoring (APM)

๔.๔.๒. Error Tracking และ Crash Reporting

๔.๔.๓. Metrics และ Logging ส่งออกไปยังระบบกลาง (เช่น Prometheus, Grafana, ELK/EFK)

๔.๔.๔. การแจ้งเตือน (Alerting) เมื่อเกิดความผิดปกติในแต่ละ Service

๔.๔.๕. มี Alerting เมื่อเกิดความผิดปกติ รวมถึง SLA/SLO ที่เกี่ยวข้องกับ mobile-backend interaction

๔.๕. รายละเอียดอื่น ๆ อ้างอิงตาม ภาคผนวก ค การพัฒนาระบบ

๕. การทดสอบและคุณภาพ (Testing & Quality Assurance)

๕.๑. ผู้รับจ้างต้องมีการทดสอบที่ครอบคลุมดังนี้

๕.๑.๑. Unit Test ครอบคลุม ≥ ๘๐% ของโค้ด

๕.๑.๒. Integration Test ครอบคลุมการเชื่อมต่อกับ API / Backend และการจัดการ token/refresh/PKCE

๕.๑.๓. UI/UX Test บนอุปกรณ์จริง (Real Device) และ Emulator

๕.๑.๔. Security Test ตาม OWASP MSTG ตาม OWASP MASTG/MASVS (ระบุระดับ L2 สำหรับข้อมูลอ่อนไหว)

๕.๑.๕. Performance Test ตรวจสอบ Response Time, Memory, Battery Usage, network reliability

๕.๑.๖. Compatibility Test ครอบคลุม Android และ iOS (๒ เวอร์ชันหลักล่าสุด)

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

๕.๑.๗. Penetration Test (Mobile App Security Assessment) โดยผู้เชี่ยวชาญภายนอก ตามภาคผนวก ช การทดสอบเจาะระบบ

๕.๒. การทดสอบต้องดำเนินการบนอุปกรณ์จริง ที่ครอบคลุมยี่ห้อ/รุ่นที่นิยม เช่น Samsung, OPPO, Xiaomi, Apple และ Tablet (iPad, Android Tablet รุ่นหลักที่มีผู้ใช้งานแพร่หลาย)

๕.๓. Security Automation

๕.๓.๑. ใช้ Mobile App Security Scanners (เช่น MobSF)

๕.๔. Dynamic Analysis

๕.๔.๑. ตรวจสอบ Runtime Behavior, Memory Leak, API Call

๕.๕. Penetration Test

๕.๕.๑. ต้องทำตาม OWASP MSTG L2 อย่างน้อย

๕.๕.๒. ต้องมี Remediation Plan และ Retest หลังแก้ไข

๕.๖. Automation & Tooling

๕.๖.๑. ใช้ Mobile App Security Scanners (เช่น MobSF) สำหรับ static/dynamic analysis

๕.๖.๒. Dynamic Analysis: ตรวจ runtime behavior, memory leak, API call, certificate pinning/ATS/Network Security Config ทำงานถูกต้อง

๕.๗. Accessibility

๕.๗.๑. UX/UI ต้องเป็นไปตาม WCAG 2.2 ระดับ AAA เป็นอย่างน้อย และรวมการตรวจนี้ไว้ในแผนทดสอบ

๖. การเผยแพร่แอปพลิเคชัน (Application Distribution & Store Deployment)

๖.๑. การนำแอปพลิเคชันขึ้น Apple App Store และ Google Play Store ต้องดำเนินการภายใต้มาตรฐานความปลอดภัย (Security Compliance) ที่กำหนดโดยแต่ละแพลตฟอร์ม เช่น

๖.๑.๑. App Store Review Guidelines (Apple), App Privacy Details (Privacy Manifests/SDK signatures/Privacy Nutrition Labels)

๖.๑.๒. Google Play Developer Policy (Google), Data safety form

๖.๒. กระบวนการ Build, Signing และ Deployment ต้องถูกจัดการผ่าน CI/CD Pipeline แบบอัตโนมัติ (Automated Release Pipeline) โดยมีขั้นตอนตรวจสอบความปลอดภัย (Security Gate) ก่อนการเผยแพร่จริง

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา

๖.๓. การสร้างและใช้งาน บัญชี Developer อย่างเป็นทางการ (Official Developer Account) ต้องอยู่ภายใต้ชื่อของ ผู้ว่าจ้าง (Client/Organization) ไม่ใช่บัญชีของผู้รับจ้าง พร้อมกำหนด RBAC และ Approval Workflow ก่อน release เพื่อให้ผู้ว่าจ้างเป็นเจ้าของสิทธิ์ในระบบทั้งหมด

๖.๔. ผู้รับจ้างต้องจัดทำ เอกสารและคู่มือการเผยแพร่ (App Deployment Guide) เพื่อให้ผู้ว่าจ้างสามารถดูแลและอัพเดตแอปในอนาคตได้เองอย่างปลอดภัย

๖.๕. ต้องมีการกำหนด การจัดการสิทธิ์ (Role-based Access Control – RBAC) บนบัญชี Developer เพื่อป้องกันการเข้าถึงโดยมิชอบ เช่น จำกัดสิทธิ์เฉพาะผู้ที่ได้รับอนุญาตจากผู้ว่าจ้าง

๖.๖. Deliverables ต้องรวมเอกสารแนวทางกรอก Privacy/Compliance (App Store Privacy Details, Google Play Data safety) และหลักฐานการตรวจความถูกต้องของข้อมูลที่กรอก

๖.๗. ต้องมี กระบวนการตรวจสอบและอนุมัติ (Approval Workflow) ก่อนการ Release แอปทุกครั้ง

๗. สิ่งที่ต้องส่งมอบ (Deliverables)

๗.๑. Source Code และ Technical Documentation

๗.๒. Security Test Report (ตาม OWASP MSTG)

๗.๓. Penetration Test Report และ Risk Mitigation Plan

๗.๔. Test Plan & Test Result ครอบคลุมทุกการทดสอบ

๗.๕. Application Package สำหรับติดตั้ง

๗.๖. คู่มือผู้ใช้งาน (User Manual)

๗.๗. คู่มือผู้ดูแลระบบ (Admin/Technical Guide)

คณพศ หงสวรางกูร ปริญญา เพ็ญไพรัตน์กุล ธีรยุทธ วัฒนะธรรมศิริ ศิร์รัฐ ศรีสุนทรพินิต สาลิเดช สัมฤทธิ์
มธุรส ไพบูลย์วรชาติ วิมลมาศ วัฒนจรูญโรจน์ รัฐธรรม ชวนเชย พันธุ์นิชิต โปษยานนท์ นัฐพล สีสวย
วิชาญ จินดารัตน์ สิทธิศักดิ์ ไชยสุข อำนาจวิทย์ หมู่ศิลป์ จุฑามาศ วงศ์เหมอนันต์ ทักษิณ หลังสตา