Mobile Application Encryption Implementation Guide

This document outlines essential guidelines and best practices for implementing encryption in mobile applications.

1. Introduction

Encryption is vital for protecting sensitive data in mobile applications. It ensures confidentiality, integrity, and security of user information stored on devices or transmitted over the network.

2. Types of Data to Encrypt

- User credentials and authentication tokens
- Personal identifiable information (PII)
- Financial and payment data
- Health and sensitive records
- Any confidential business logic or data

3. Storage Encryption

1. Use platform-provided secure storage, such as:
   - **iOS:** Keychain, Data Protection API
   - **Android:** Keystore, EncryptedSharedPreferences

2. Encrypt databases using libraries:
   - Use SQLCipher or Room Database encryption (Android)
   - Enable built-in database encryption (CoreData, Realm, etc.)

3. Never store secrets or keys in plain text on the device.

4. Data-in-Transit Encryption

1. Always use HTTPS/TLS for all network communications.
2. Implement certificate pinning to prevent MITM attacks.
3. Avoid using weak ciphers or insecure protocols (e.g., SSLv3, TLS 1.0).

5. Key Management

- Generate and store cryptographic keys using secure platform APIs.
- Rotate keys regularly.
- Do not hardcode keys in source code or resources.

6. Recommended Algorithms

- **Symmetric:** AES-256-GCM
- **Asymmetric:** RSA-2048 or higher, ECC
- **Hashing:** SHA-256, SHA-3

7. Example: Encrypt/Decrypt (Pseudo-code)

```
key = generateSecureKey()
cipherText = encrypt(data, key)
plainText = decrypt(cipherText, key)
```

8. Additional Best Practices

- Apply secure coding standards (e.g., OWASP MASVS).
- Perform regular security testing and code reviews.
- Monitor for vulnerabilities in third-party libraries.
- Educate developers on secure coding and encryption usage.

Disclaimer: This guide provides general recommendations. Always tailor security measures to your application's specific requirements and regulatory standards.