Secure Offline QR Code System – RFC v1.1

Abstract

This document specifies a Secure Offline QR Code system inspired by observed UIDAI Secure QR behavior. It defines encoding rules, cryptographic verification, and a full Flutter mobile application implementation for scanning, decoding, and verifying QR-contained data without any network dependency.

1. Observed UIDAI Secure QR Behavior

Based on Android logcat analysis, UIDAI Secure QR embeds all demographic data directly in the QR payload. Fields are UTF-8 encoded, separated by 0xFF bytes, followed by embedded JPEG photo data and an RSA digital signature. Verification is performed entirely offline using a bundled public key.

2. Binary Encoding Rules

• Text encoding: UTF-8
• Field separator: 0xFF (255)
• Photo: JPEG binary
• Signature: RSA-2048
• Order: Fixed positional fields
• QR size target: < 3 KB

3. Cryptography

• Algorithm: RSA-2048
• Hash: SHA-256
• Padding: PKCS#1 v1.5
• Verification: Offline using public key embedded in app
Private keys MUST NEVER be shipped in mobile applications.

4. Flutter Application Architecture

Modules:
scanner/ – QR scanning using mobile_scanner
decoder/ – Base64 decoding, 0xFF splitting
crypto/ – RSA signature verification (pointycastle)
ui/ – Data rendering and verification status

5. Flutter Implementation – Step by Step

Step 1: Create project using flutter create
Step 2: Configure Android/iOS camera permissions
Step 3: Integrate mobile_scanner for QR detection
Step 4: Decode Base64 payload to Uint8List
Step 5: Split byte stream using 0xFF separators
Step 6: Extract payload and signature
Step 7: Verify signature using RSA public key
Step 8: Parse fields and render UI

6. UIDAI-Compatible Parsing Logic

Block indices map to specific demographic fields (name, DOB, gender, address). Reserved blocks must be preserved. JPEG photo bytes are rendered using Image.memory.

7. Failure Modes

• Signature mismatch → Reject QR
• Invalid Base64 → Reject QR
• Missing blocks → Reject QR
• Oversized QR → Reject QR

8. Security & Privacy

• No Aadhaar number present
• No network calls
• Tamper detection via signature
• Offline-first trust model

9. Extensions

Optional enhancements include payload encryption, expiry timestamps, revocation lists, and version negotiation.

Conclusion

This RFC v1.1 serves as both a protocol specification and a Flutter engineering guide, enabling developers to build secure, offline-verifiable QR systems compatible with UIDAI Secure QR principles.