Cryptography Standards Checklist

Approved algorithms, TLS config, and key management

Algorithm Selection

- ■ Symmetric encryption: AES-256-GCM (approved) — NOT DES, 3DES, RC4
- ■ Hashing: SHA-256/SHA-384/SHA-512 — NOT MD5, SHA-1
- ■ Key exchange: ECDH with P-256/P-384 or X25519
- ■ Digital signatures: ECDSA, Ed25519, or RSA-PSS (min 2048-bit)
- ■ Password hashing: Argon2id, bcrypt, or scrypt — NOT PBKDF2-SHA1

TLS Configuration

- ■ TLS 1.3 preferred, TLS 1.2 minimum — NO TLS 1.0/1.1, NO SSL
- ■ Strong cipher suites only (AEAD ciphers)
- ■ HSTS header enabled with min 1-year max-age
- ■ Certificate pinning considered for mobile/API clients
- ■ Certificate chain validated and monitored for expiry

Key Management

- ■ Keys stored in HSM or key management service (not in code)
- ■ Key rotation schedule defined and automated
- ■ Key access logged and auditable
- ■ Separate keys per environment (dev/staging/prod)
- ■ Emergency key revocation procedure documented and tested