CBOM TEMPLATE FOR MOBILE APPS

CRYPTOMATHiC

Entry guidance: If it has its own lifecycle (created, stored, used, rotated/expired), it deserves its own row

	Placeholder/Guiding Text to Fill Out:	Asset ID (1)	Asset ID (3)	Asset ID (3)
Key Type	e.g., Runtime key / Device key / Certificate / Token / App signing key / Server key / Platform-managed. Pick one category per row.			
Key Name	Unique name/alias used in code, keystore, HSM, or config (match implementation where possible).			
Purpose	What this protects and where it's used (e.g., "encrypt cached account data", "sign transaction approval").			
Algorithm	Specify algorithm + parameters (e.g., AES-256-GCM, ECDSA secp256k1, RSASSA-PSS SHA-256, HKDF-SHA256). Include key size/curve/mode.			
Generation Location	Where it is created (e.g., iOS Secure Enclave, Android Keystore/TEE, Server HSM, CI/CD signing service, Vendor service).			
Storgae	Where it lives at rest/in use (e.g., Keychain/Keystore, HSM, encrypted file, memory-only, OS-managed). Note exportability if relevant.			
Lifetime	Ephemeral vs persistent + cryptoperiod (e.g., "per session", "90 days", "until cert expiry"). Include expiry/renewal cadence if known.			
Risk Level	Low / Medium / High / Critical — based on impact if compromised + exposure + feasibility (add a short rationale if helpful).			
Recommended Mitigations	Controls to reduce risk (e.g., hardware-backed non-exportable keys, least privilege, attestation, step-up auth, monitoring, short token TTL, secure deletion).			
Rotation Mechanism (how, by whom, how fast)	Describe the process + owner + trigger + SLA (e.g., "Automated weekly rotation by platform team; emergency rotation within 24h").			
PQC Impact	Mark: No change / Review / Migrate to PQC / Hybrid recommended. Note dependency (TLS/signing/tokens) + target timeframe.			