

AI Agent Protocol & Instructions (AGENTS.md)

Guidelines for Autonomous Agent Code Reuse & Monorepo Integration

Repository: <https://github.com/sh15aa/Appreusable> Total Modules: 163 Status:
Production-Grade

REUSABLE CODE LIBRARY: MOBILE PRODUCT FACTORY

This repository contains **163 production-grade, hardened, reusable modules** for building cross-platform mobile products (Flutter for iOS & Android), isolated backend services (FastAPI), zero-trust security architectures, and enterprise scale infrastructures.

Repository: <https://github.com/sh15aa/Appreusable>

Branch: **main**

■■ CORE RULE FOR AI AGENTS

Before generating ANY new code, boilerplate, architecture, or features for any product or application:

1. **SEARCH FIRST:** Check [[registry/modules.json](#)](file:///home/shiva/appreusable/registry/modules.json) or run `/tools/factory-pull search <keyword>`.
2. **INSPECT:** Read the module's [README.md](#) and check its interface in [lib/](#) or [app/](#).
3. **REUSE:** Integrate or import the existing module.
4. **DO NOT REINVENT:** Never recreate authentication, state management, encryption, HTTP networking, local storage, payments, or security features from scratch.

■ PRIORITY HIERARCHY

Existing Reusable Module in this Library ▼ Existing Application Feature Adaptation ▼ New Implementation (Only if no module covers the requirement)

■ MODULE CAPABILITIES INDEX (163 Modules)

1. Architecture & Core Mobile (Mod 01 - 10)

- `mod_01_product_idea_engine`: Viability scoring, market validation FSM.
- `mod_02_tech_stack_standard`: Strict Dart linter rules, clean architecture boundaries.
- `mod_03_app_starter_template`: Production Flutter starter template with DI.
- `mod_04_core_architecture`: `Result<S, F>`, `UseCase<Type, Params>` zero-exception foundation.
- `mod_05_app_config_system`: Strongly-typed multi-environment configuration (Dev/Staging/Prod).
- `mod_06_android_identity`: 4096-bit RSA keystore generation, ProGuard/R8 obfuscation.
- `mod_07_ios_identity`: Hardened `Info.plist`, ATS enforcement, Entitlements.
- `mod_08_environment_system`: Encrypted `.env` manager with schema validation.

- [mod_09_auth_module](#): PKCE OAuth2, JWT rotation, biometric & hardware keystore backing.
- [mod_10_authorization_system](#): Zero-trust granular RBAC permission engine.

2. Data, Offline & UI Design System (Mod 11 - 20)

- [mod_11_local_data_system](#): Encrypted KV & SQLCipher database with keystore encryption.
- [mod_12_offline_first_sync](#): Outbox pattern sync with UUIDv4 idempotency keys.
- [mod_13_api_layer](#): Resilient HTTP client with SSL pinning, jittered retry, [ApiResponse<T>](#).
- [mod_14_error_handling](#): Centralized error taxonomy; scrubs stack traces and PII.
- [mod_15_state_management](#): Standardized state machine ([Loading](#), [Success](#), [Error](#), [Empty](#), [Offline](#)).
- [mod_16_design_system](#): Atomic UI components ([AppButton](#), [AppCard](#), [AppTextField](#), [AppSkeleton](#)).
- [mod_17_design_tokens](#): Spacing, radius, elevation, typography, and color scales.
- [mod_18_responsive_ui](#): Adaptive breakpoints for phones, foldables, and tablets.
- [mod_19_accessibility](#): WCAG 2.1 AA/AAA contrast and minimum 48x48dp touch targets.
- [mod_20_dark_mode](#): Dynamic theme engine: System, Light, Dark, AMOLED.

3. Hardware, AI & Monetization (Mod 21 - 30)

- [mod_21_device_features](#): Haptics, Secure Clipboard (auto-clears in 60s), Biometrics bridge.
- [mod_22_permission_architecture](#): Zero-crash permission manager with rationale dialogs.
- [mod_23_push_notifications](#): FCM / APNs push handler with encrypted payloads.
- [mod_24_analytics](#): Privacy-first analytics; scrubs PII, GDPR consent mode.
- [mod_25_crash_monitoring](#): Sentry / Crashlytics wrapper with rolling breadcrumbs.
- [mod_26_performance_monitoring](#): Startup duration, screen render latency, API timing watchdog.
- [mod_27_ai_client_module](#): Mobile AI client with SSE streaming and prompt hydration.
- [mod_28_ai_cost_gateway](#): Token budgeting, user tier quotas, rate-limiting, model fallbacks.
- [mod_29_subscription_system](#): Cross-platform IAP (StoreKit 2, Google Play Billing, RevenueCat).
- [mod_30_purchase_security](#): Server-side receipt verification and HMAC-SHA256 webhooks.

4. Growth, Deep Links & Lifecycle (Mod 31 - 40)

- [mod_31_ads_module](#): Privacy-friendly ads with frequency capping and remote kill-switch.
- [mod_32_remote_config](#): Remote configuration client with local cache fallbacks.
- [mod_33_feature_flags](#): Deterministic SHA-256 user hashing for gradual rollouts.
- [mod_34_deep_link_system](#): Universal & App Links router with URI validation.
- [mod_35_sharing_system](#): Native share sheet integration & attribution tracking.
- [mod_36_viral_loops](#): Cryptographic referral codes and reward unlock engine.
- [mod_37_onboarding_engine](#): Multi-step onboarding state machine with permission priming.
- [mod_38_app_lifecycle](#): Lifecycle observer with state flush before suspension.
- [mod_39_security_hardening](#): Root/Jailbreak detection, anti-emulator, anti-debugger.
- [mod_40_data_validation](#): Strict input sanitization, anti-SQLi, anti-XSS escaping.

5. Backend, Storage & QA (Mod 41 - 50)

- [mod_41_database_architecture](#): Encrypted SQLite migration engine with atomic rollbacks.
- [mod_42_file_storage](#): Presigned URL cloud upload manager with MIME & size validation.
- [mod_43_background_jobs](#): Battery-optimized background scheduler with power/network constraints.
- [mod_44_app_backend_template](#): Zero-trust FastAPI backend with JWT validation & isolated DB.
- [mod_45_cicd_factory](#): Fastlane & GitHub Actions pipelines for automated AAB & IPA releases.

- [mod_46_automated_testing](#): Unit test harness, MockWebServer, and test fixtures.
- [mod_47_golden_user_journey](#): Maestro / Patrol E2E automation for conversion funnels.
- [mod_48_device_test_matrix](#): Matrix covering 12 device archetypes across Android and iOS.
- [mod_49_release_checklist](#): 32-criteria automated pre-flight release auditor.
- [mod_50_aso_factory](#): App Store Optimization metadata engine and validator.

6. Factory Tooling & Synthesis (Mod 51 - 63)

- [mod_51_screenshot_factory](#): Automated multi-device screenshot capture and 5-slide layout builder.
- [mod_52_review_monitoring](#): Review sentiment scraper (Bugs, Pricing, Feature Requests).
- [mod_53_analytics_dashboard](#): Aggregates DAU, MAU, Retention, and MRR.
- [mod_54_health_scorecard](#): Product health evaluator (Grades A-D).
- [mod_55_app_factory_db](#): SQLite portfolio database managing all product definitions.
- [mod_56_automated_cli](#): [factory-cli](#): 1-command product scaffolding tool.
- [mod_57_ai_agent_team](#): Prompt specifications for 15 specialized product agents.
- [mod_58_dev_pipeline](#): 16-phase gatekeeper pipeline with strict transition criteria.
- [mod_59_architecture_boundary](#): AST linter ensuring modules remain product-agnostic.
- [mod_60_portfolio_registry](#): Melos monorepo orchestrator for portfolio dependency management.
- [mod_61_isolation_guardian](#): Rule 61: Strict per-product isolation (Zero shared DBs).
- [mod_62_one_click_synthesizer](#): Rule 62: Autonomous 'One-Click' generator (PRD, OpenAPI, Schema, App & Backend).
- [mod_63_master_checklist_tracker](#): Rule 63: 360+ task checklist CLI tracker across 10 layers & 16 phases.

7. Zero-Trust Security, AuthZ, Secrets & Tenancy (Mod 64 - 78)

- STRIDE threat modeling ([mod_64](#)), zero-trust boundary ([mod_65](#)), zero-trust API chain ([mod_66](#)).
- OWASP API defenses: BOLA ([mod_67](#)), BOPLA ([mod_68](#)), Function-level authorization ([mod_69](#)).
- Admin security & MFA ([mod_70](#)), Break-glass access ([mod_71](#)), Vault secrets ([mod_72](#)), Secret rotation ([mod_73](#)), Key management DEK/KEK ([mod_74](#)).
- Database security TLS/roles ([mod_75](#)), Tenancy isolation ([mod_76](#)), Backup recovery test ([mod_77](#)), Disaster recovery RPO/RTO ([mod_78](#)).

8. Scale, Abuse Defense & Integrity (Mod 79 - 96)

- Multi-region architecture ([mod_79](#)), Autoscaling policies ([mod_80](#)), Load shedding ([mod_81](#)).
- Circuit breaker ([mod_82](#)), Retry idempotency ([mod_83](#)), Rate limiting matrix ([mod_84](#)).
- Abuse prevention ([mod_85](#)), Bot defense ([mod_86](#)), Replay attack protection ([mod_87](#)).
- Session security ([mod_88](#)), Token security ([mod_89](#)), Device secure storage ([mod_90](#)).
- App integrity Play Integrity/App Attest ([mod_91](#)), Anti-tamper resilience ([mod_92](#)), TLS pinning ([mod_93](#)).
- Webhook signature validation ([mod_94](#)), File upload security ([mod_95](#)), SSRF protection ([mod_96](#)).

9. I/O Security, Audit & Supply Chain (Mod 97 - 115)

- Input security ([mod_97](#)), Output escaping ([mod_98](#)), Error leak prevention ([mod_99](#)).
- Security logging ([mod_100](#)), Audit logging ([mod_101](#)), SIEM monitoring ([mod_102](#)), Alerting ([mod_103](#)).
- Incident response ([mod_104](#)), Emergency controls ([mod_105](#)), Force upgrade ([mod_106](#)), Remote kill-switch ([mod_107](#)).
- Supply chain security ([mod_108](#)), SBOM generation ([mod_109](#)), Dependency policy ([mod_110](#)).
- Secure build environment ([mod_111](#)), Reproducible builds ([mod_112](#)), Artifact signing ([mod_113](#)), CI/CD security ([mod_114](#)), Branch protection ([mod_115](#)).

10. SAST/DAST, Privacy & Cloud Infrastructure (Mod 116 - 145)

- Static analysis SAST ([mod_116](#)), Dynamic analysis DAST ([mod_117](#)), Penetration testing ([mod_118](#)).
- OWASP MASVS v2.0 verification ([mod_119](#)), Secret scanning ([mod_120](#)), Vulnerability management ([mod_121](#)).
- Privacy by design ([mod_122](#)), GDPR/CCPA data export ([mod_123](#)), Right to be forgotten ([mod_124](#)), Data retention ([mod_125](#)).
- Third-party risk ([mod_126](#)), Open source license compliance ([mod_127](#)), Vendor lock-in defense ([mod_128](#)).
- Cost explosion prevention ([mod_129](#)), FinOps attribution ([mod_130](#)), Observability metrics ([mod_131](#)).
- Distributed tracing ([mod_132](#)), Real user monitoring ([mod_133](#)), Synthetic monitoring ([mod_134](#)).
- Health check endpoints ([mod_135](#)), SLA monitoring ([mod_136](#)), API documentation OpenAPI ([mod_137](#)).
- API versioning ([mod_138](#)), API inventory ([mod_139](#)), Edge security headers ([mod_140](#)).
- DDoS resilience ([mod_141](#)), Network segmentation ([mod_142](#)), Cloud IAM least privilege ([mod_143](#)).
- Environment isolation ([mod_144](#)), Production data protection ([mod_145](#)).

11. Scale Gate, Fraud & Security Monitoring (Mod 146 - 163)

- Support tool security ([mod_146](#)), Social engineering defense ([mod_147](#)), Fraud detection ([mod_148](#)).
- Release rollback ([mod_149](#)), Canary releases ([mod_150](#)), Feature-gated migrations ([mod_151](#)).
- Security regression suite ([mod_152](#)), Security scorecard gate ([mod_153](#)), Release gatekeeper ([mod_154](#)).
- 1M User scale gate ([mod_155](#)), Capacity planning ([mod_156](#)), Chaos testing ([mod_157](#)), Business continuity ([mod_158](#)).
- Vulnerability disclosure ([mod_159](#)), Security patch pipeline ([mod_160](#)), Blast radius control ([mod_161](#)).
- Central factory security monitor ([mod_162](#)), Final production architecture ([mod_163](#)).

■ NEVER DO

- Never rewrite authentication, database encryption, networking, or security from scratch.
- Never duplicate an existing reusable module.
- Never hardcode secrets, API keys, or credentials.
- Never violate Rule 61: Keep app databases and backends completely isolated.
- Never assume compatibility without checking the module README and dependencies.