OBSIDIAN CIRCUIT

OBSIDIAN CIRCUIT

TECHNICAL PRODUCT MEMORANDUM

ONYX

CODENAME:

VALKYRJA

INTELLIGENCE-GRADE MOBILE COMPUTING PLATFORM

DOCUMENT TYPE	Technical Product Memorandum — Manufacturer & Supplier Brief
DOCUMENT VERSION	1.0 — Initial Release
PREPARED BY	Desirae Stark, Chief Architect
ORGANIZATION	Obsidian Circuit
DATE	April 2026
CLASSIFICATION	PROPRIETARY & CONFIDENTIAL
TARGET AUDIENCE	Hardware Manufacturers, Component Suppliers, Software Integration Teams

EXECUTIVE SUMMARY

Product Vision & Strategic Context

Purpose. This memorandum constitutes the authoritative technical specification for Onyx (Codename: VALKYRJA), a purpose-engineered mobile computing platform developed by Obsidian Circuit under the QWAMOS operating system architecture. It is intended to provide hardware manufacturers, component suppliers, and software integration partners with the complete specification required to procure, fabricate, assemble, and validate the device.

Mission. VALKYRJA is the world's first commercial mobile device to deliver intelligence-grade operational security as the default user experience — not as a configuration layer, not as a third-party add-on, but as the foundational architecture from which all other capabilities are derived. The device targets a market gap that no existing flagship addresses: a phone that simultaneously exceeds all commercial flagships in raw computational performance, matches their user experience quality, and provides security capabilities previously available only through classified government platforms.

Differentiation. Every current 'secure phone' sacrifices performance or usability to achieve security. Every current flagship sacrifices security to achieve performance and UX. VALKYRJA is architected to deliver all three simultaneously through a layered approach: hardware isolation enforced at silicon level, post-quantum cryptography throughout the full stack, a KVM hypervisor providing VM-level compartmentalization, and a consumer-grade UX abstraction layer that makes the complexity invisible to the end user.

Operating System. VALKYRJA ships exclusively with QWAMOS v3.1.0+ (Qubes+Whonix Advanced Mobile Operating System), an open-source (AGPL-3.0) ARM64-native hypervisor OS with 27 completed development phases, 50,000+ lines of code, and full post-quantum cryptographic hardening throughout the stack.

Market Tiers

Tier	Designation	Target Market
Tier 1	Consumer Privacy	Privacy-conscious consumers, journalists, executives requiring corporate data separation. Volume production device.
Tier 2	Professional Security	Security researchers, legal professionals, enterprise mobile security, financial institutions, diplomatic corps.
Tier 3	Operational	Intelligence community adjacent, government contractors, cleared personnel. Custom configuration per deployment.

Performance Targets vs. Market Comparators

Capability	VALKYRJA	Samsung Galaxy S26 Ultra	Google Pixel 10 Pro XL
Hypervisor OS	Native KVM — full Type-1	None	AVF/pKVM (limited)
RAM	32 GB LPDDR5X	12–16 GB LPDDR5X	16 GB LPDDR5X
Internal Storage	1 TB UFS 4.0 + 512 GB UFS 4.0	256 GB – 1 TB	128 GB – 1 TB
Privacy Display	FMP LEAD 2.0 + FLAG_SECURE (dual enforcement)	FMP LEAD 2.0 (software only)	None
Network Anonymization	Mandatory Tor/I2P all traffic	None	None
PQC Cryptography	Full stack — all comms, storage, keys	None	Partial
Hardware Kill Switches	4× physical relay	None	None
Security Microcontroller	Discrete HSM + nuclear-powered HNCP	TrustZone only	Titan M2
VM Isolation	8 isolated domains	App sandbox	App sandbox
Charge Time (0→100%)	6–10 min (graphene cell)	~80 min	~70 min

SECTION 1 — COMPUTE & PROCESSING ARCHITECTURE

Primary SoC, GPU, NPU, and Supporting Silicon

1.1 Primary System-on-Chip: Rockchip RK3588

The primary compute engine is the Rockchip RK3588, selected as the sole ARM64 SoC in the market that satisfies the non-negotiable requirement of full EL2 (Exception Level 2) hypervisor access, enabling native KVM virtualization. This property — absent from all Qualcomm Snapdragon, Samsung Exynos, and MediaTek Dimensity SoCs due to proprietary hypervisor firmware occupying EL2 — is fundamental to QWAMOS's security architecture and cannot be substituted.

Designation	Rockchip RK3588
Process Node	8nm FinFET (Samsung Foundry)
CPU Cluster A	4× ARM Cortex-A76 @ 2.4 GHz
CPU Cluster B	4× ARM Cortex-A55 @ 1.8 GHz
CPU Architecture	ARM DynamIQ big.LITTLE, ARMv8.2-A ISA
Total CPU Cores	8 (Octa-core)
L2 Cache (A76)	1 MB per core (4 MB total)
L2 Cache (A55)	512 KB per core (2 MB total)
L3 Cache	3 MB shared
GPU	ARM Mali-G610 MP4 (4-core), OpenGL ES 3.2, Vulkan 1.2, OpenCL 2.2
GPU Clock	Up to 1,000 MHz
NPU	6 TOPS (Tera Operations Per Second), 3-core neural processor
VPU	8K@60fps decode; 8K@30fps encode; AV1, H.265, H.264, VP9
ISP	Dual-core ISP, up to 48 MP + 48 MP simultaneous
Memory Interface	64-bit LPDDR4/LPDDR5, dual-channel
Max Memory Bandwidth	68.3 GB/s (LPDDR5 @ 4266 MHz)
PCIe	2× PCIe 3.0 x4 + 1× PCIe 2.0 x1
USB	USB 3.1 Gen1 + USB 2.0 OTG
EL2 / KVM	CONFIRMED — kernel boots at EL2, /dev/kvm accessible
TDP	~10–14 W peak; ~4–8 W mobile thermal envelope

1.2 CPU Architecture & QWAMOS VM Allocation

VM Domain	CPU Allocation	Priority	Notes
Dom0 / Control VM	1× A76 + 2× A55 (reserved)	Highest — realtime	ML threat detection, VM lifecycle, security policies
Gateway VM (Tor/I2P)	1× A76 + 1× A55 (dedicated)	High — sustained	Always-on; Tor circuits, I2P, DNSCrypt, behavioral obfuscation
Active User VM	2× A76 + 1× A55 (primary burst)	High — interactive	Android VM, Arch VM, or Kali VM — whichever profile is active
Background VMs	Remaining A55 cores	Low — background	Suspended or minimal-activity domains
AI Governor	NPU (6 TOPS) — dedicated	Asynchronous	ML resource scheduling, threat detection, LLM inference

VM Domain	CPU Allocation	Priority	Notes
GPU Isolation	Mali-G610 MP4 — per-VM sliced	As-needed	Vulkan passthrough per VM; no cross-VM GPU access

1.3 Supporting Security Silicon

Component	Specification
Discrete HSM	Infineon SLB 9672 TPM 2.0 — dedicated post-quantum key management, attestation, ML-DSA-87 operations. Communicates via SPI to RK3588; key material never exported in plaintext.
Hardware TRNG	Dedicated true random number generator IC — ring oscillator entropy + reverse-biased junction shot noise. Seeds HSM, KVM hypervisor entropy pool, and all VM-level key generation. v1 baseline entropy source.
Glass Photonic QRNG (v2)	Borosilicate glass photonic chip fabricated by femtosecond laser direct writing (FLDW) on Corning EAGLE XG substrate. Entropy source: quantum vacuum fluctuations measured by CV heterodyne receiver at 1550 nm. Demonstrated: 42.7 Gbit/s secure random bit generation; CMRR >73 dB; ~1 dB insertion loss; 8+ hour field stability without recalibration; polarization-independent. No cleanroom required — fabricated by femtosecond laser into commercially available glass. Targets NIST SP 800-90B entropy source certification. Replaces classical TRNG in v2 hardware platform.
HNCP	Ultra-low-power RISC-V microcontroller (<40 µW). Sits physically on-wire between cellular modem and RK3588. Enforces traffic isolation rules in hardware. Powered by dedicated nuclear security rail.
Tamper Detection MCU	ARM Cortex-M0+ (STM32L0 class, <1 µW stop mode). Monitors physical tamper conditions. Powered by nuclear security rail. Triggers key destruction on tamper confirmation.
Biometric Enclave	Discrete ARM SecurCore SC300 — dedicated fingerprint template storage and matching. Communicates result only (match/no-match) over hardened interface.
Secure Boot Chain	Custom U-Boot bootloader with verified boot (AVB2.0), hardware root of trust anchored in HSM. Kernel signature verified before EL2 handoff.

■ KVM/EL2 REQUIREMENT — NON-SUBSTITUTABLE
The RK3588 is specified due to its confirmed EL2 access for native KVM. NO substitution with Qualcomm Snapdragon, Samsung Exynos, or MediaTek Dimensity SoCs is acceptable. Any proposed SoC substitution must provide documented EL2 access confirmation before evaluation.

SECTION 2 — MEMORY ARCHITECTURE

Maximum RAM Configuration & Allocation

2.1 Primary RAM — LPDDR5X

Total Capacity	32 GB LPDDR5X (maximum supported by RK3588 memory controller)
Standard	LPDDR5X — JEDEC JESD209-5B
Data Rate	8,533 Mbps per pin
Interface Width	64-bit dual-channel
Peak Bandwidth	68.3 GB/s
Package	PoP (Package-on-Package) or discrete FBGA — integrated with SoC
Operating Voltage	0.5V (VDDQ) — ultra-low power LPDDR5X spec
ECC	Optional inline ECC — recommended for Dom0 / HSM communication channels
Temperature Range	0°C to 85°C (commercial); -20°C to 85°C (extended industrial option)
Preferred Suppliers	Samsung Semiconductor (K4X), SK Hynix (H58G), Micron (MT62F)

2.2 VM Memory Allocation Budget

VM Domain	Base Allocation	Max Burst	Purpose
Dom0 / Control VM	2 GB	4 GB	Hypervisor management, ML detection models, security policies
Gateway VM	2 GB	3 GB	Tor daemon, I2P daemon, DNSCrypt, VPN, WebTunnel, V2Ray, behavioral obfuscation ML
Android VM (Primary)	6 GB	10 GB	Primary user Android environment, app ecosystem, daily use
Secure VM (Arch Linux)	4 GB	6 GB	PQC communications, Signal+ZRTP, steganography, secure file operations
Kali NetHunter VM	3 GB	5 GB	Offensive security, penetration testing, vulnerability assessment
Vault VM (Air-gapped)	1 GB	2 GB	Key storage, cryptographic operations — no network interface
Ubuntu Dev VM	2 GB	4 GB	Development environment, AI App Builder pipeline
Disposable VM	2 GB	4 GB	Ephemeral — fresh instantiation per session, auto-wipe on close
Kernel / Hypervisor overhead	2 GB	2 GB	KVM hypervisor, VirtIO drivers, NIC enforcer, GPU manager
Dynamic Pool	6 GB	6 GB	Burst buffer, snapshot staging, model loading, ML inference staging
TOTAL	32 GB	—	Full platform allocation — no swap partition; all ops in encrypted RAM

SECTION 3 — STORAGE ARCHITECTURE

Maximum Capacity, UFS 4.0, Encrypted Volume Stack

3.1 Primary Storage — UFS 4.0

Capacity	1 TB UFS 4.0 (primary)
Standard	JEDEC UFS 4.0 (JESD220F)
Sequential Read	Up to 4,200 MB/s
Sequential Write	Up to 2,800 MB/s
Random Read (4K)	Up to 100,000 IOPS
Random Write (4K)	Up to 70,000 IOPS
Interface	UniPro / M-PHY Gen5 — PCIe 4.0 equivalent bandwidth
Encryption	Hardware AES-256 inline encryption at UFS controller level (baseline layer)
Preferred Suppliers	Samsung Semiconductor (KLUDG), SK Hynix (H28U1), Micron (MTFC)

3.2 Secondary Storage — PCIe NVMe

Capacity	512 GB NVMe SSD (secondary — PCIe 3.0 x4)
Interface	PCIe 3.0 x4 via RK3588 PCIe controller
Sequential Read	Up to 3,500 MB/s
Sequential Write	Up to 3,000 MB/s
Assignment	Dedicated to Vault VM encrypted volume — air-gapped from network VMs
Encryption	QWAMOS PQC Volume (ML-KEM-1024 + ChaCha20-Poly1305) on top of hardware AES

3.3 Storage Allocation Map

Volume	Capacity & Assignment
QWAMOS Base System (UFS)	64 GB — Hypervisor, Dom0, Gateway VM, kernel, U-Boot
Android VM Image (UFS)	200 GB — Primary Android environment, apps, media
Secure VM Image (UFS)	100 GB — Arch Linux secure comms environment
Kali NetHunter VM (UFS)	100 GB — Offensive security tools and datasets
Ubuntu Dev VM (UFS)	100 GB — Development environment and project files
Disposable VM Pool (UFS)	50 GB — Ephemeral VM instantiation pool (overwritten each session)
VM Snapshot Buffer (UFS)	150 GB — Rollback snapshots for all active VMs
Encrypted User Data (UFS)	236 GB — General encrypted user storage, accessible per profile
Vault VM Volume (NVMe)	512 GB — Air-gapped classified storage, key material, evidence logs
TOTAL USABLE	~1.5 TB across UFS + NVMe

3.4 Encryption Stack

Layer	Algorithm	Scope
Layer 1 (Hardware)	AES-256 XTS — UFS/NVMe hardware inline	All physical storage
Layer 2 (QWAMOS PQC Volume)	ML-KEM-1024 (key encapsulation) + ChaCha20-Poly1305 (AEAD)	Per-VM encrypted volumes
Layer 3 (Key Derivation)	Argon2id — GPU/ASIC-resistant KDF from passphrase	Master key derivation
Layer 4 (Key Storage)	ML-DSA-87 — hardware-backed in Infineon HSM	Key material protection
Secure Deletion	3-pass DoD-grade wipe + AES key destruction	On panic wipe / VM teardown

SECTION 4 — DISPLAY ARCHITECTURE

Samsung LEAD 2.0 FMP — Privacy Display Integration

4.1 Panel Specification

Panel Technology	Samsung Display LEAD 2.0 AMOLED with Flex Magic Pixel (FMP) — privacy display
Privacy Technology	Flex Magic Pixel — dual pixel type (Narrow + Wide) with multi-layer Black Matrix architecture
Diagonal Size	6.9 inches
Resolution	3088 × 1440 px (WQHD+)
Pixel Density	~490 PPI
Refresh Rate	1–120 Hz LTPO 4.0 adaptive
Peak Brightness	2,600 nits
Privacy Mode (45° off-axis)	3.5% front brightness retained (vs. ~40% on conventional OLED)
Privacy Mode (60° off-axis)	0.9% or less front brightness retained — screen appears black
Color Gamut	DCI-P3 > 99%, sRGB 100%
HDR	HDR10+ certified
FLAG_SECURE	Enforced at Flutter compositor level across all VM domains — no screen capture possible
Supplier	Samsung Display Corporation — LEAD 2.0 / FMP panel; direct B2B engagement required

4.2 QWAMOS Profile-Native FMP Integration

Profile	FMP State	FLAG_SECURE	Rationale
Everyday ■	Off (wide emission)	Active	Normal use; UX priority
Private ■	Standard Privacy (30° cone)	Active	Moderate threat; transaction protection
Secure ■	Maximum Privacy (tight cone)	Active	High threat; classified comms
Ghost ■	Maximum Privacy (tight cone)	Active	Hostile environment; full countersurveillance
Duress	Off (standard)	Active	Decoy profile must appear normal to coercive observer

SECTION 5 — POWER ARCHITECTURE

Four-Domain Independent Power System

5.1 Architecture Overview

Domain	Source	Powers
Domain 1 — Solar Harvesting	Perovskite QD conformal panel (rear)	Feeds Domain 2 primary cell via isolated PMIC charge path
Domain 2 — Primary Compute Cell	Graphene-silicon Li-ion + QD electrode enhancement	RK3588, all VMs, display, 5G modem, WiFi, storage, all compute
Domain 3 — Nuclear Security Rail	Betavolt BV100 betavoltaic cell	HNCP, Tamper MCU, RTC — permanently, without interruption
Domain 4 — Physical Kill Circuits	Passive — no power required	Modem RF, microphone ground short, camera power, GPS power

5.2 Primary Cell — Graphene-Silicon Li-Ion

Cell Chemistry	Graphene-silicon composite anode Li-ion (graphene-stabilized silicon anode)
Nominal Capacity	7,700 mAh effective (nominal 5,500 mAh graphene-silicon, +40% vs. standard Li-ion)
Electrode Enhancement	Graphene quantum dot (GQD) electrode additives — additional ~20% effective energy density
Effective Energy	~35 Wh total usable energy
Charge Protocol	USB Power Delivery 3.1 — up to 100W (28V/5A profile)
Charge Time	6–10 minutes at full 100W PD input
Cycle Life	2,000+ cycles to >80% capacity
Procurement	Custom cell engagement required: Lyten (US), GMG (Australia), or equivalent

5.3 Nuclear Security Rail — Betavoltaic Cell

Technology	Betavoltaic — diamond semiconductor with Nickel-63 isotope
Product Reference	Betavolt BV100 (or equivalent)
Output Power	100 µW continuous
Output Voltage	3V
Dimensions	15 × 15 × 5 mm
Operational Life	50 years (Ni-63 half-life: 100 years)
External Radiation	None (diamond matrix provides complete beta shielding)
Powers	HNCP (20–40 µW) + Tamper MCU (<1 µW) + RTC (<0.1 µW) + kill switch circuit (5 µW)
Regulatory	NRC (US) or national equivalent licensing required for radioactive isotope incorporation
Procurement	Betavolt New Energy Technology (Beijing) — direct commercial engagement

5.4 Operational Runtime Estimates

Usage Scenario	Active Systems	Net Draw	Runtime
Deep Standby	Dom0 + Gateway VM only; screen off; radios idle	~1.2 W	28–32 hours

Usage Scenario	Active Systems	Net Draw	Runtime
Tactical Standby	Full QWAMOS stack; 5G connected; periodic Tor comms	~2.1 W	14–17 hours
Light Daily Use	Screen on; 1 active VM; WiFi; browsing / messaging	~3.7 W	8–10 hours
Moderate Operational	Screen on; 2–3 VMs active; WiFi + 5G; comms active	~9.1 W	3.5–4.5 hours
Heavy Use	All VMs; screen max brightness; 5G data; crypto ops	~16.8 W	1.8–2.5 hours
Recharge (0 → 100%)	USB-C PD 100W input	—	6–10 minutes

SECTION 6 — HARDWARE SECURITY ARCHITECTURE

Silicon-Level Security — Below Software Attack Surface

6.1 Security Domain Isolation

Security Layer	Mechanism	Attack Vectors Addressed
Layer 0 — Physics	Nuclear-powered HNCP on-wire; physical kill switch circuits	Battery removal defeat; modem bypass; physical coercion
Layer 1 — Silicon	Discrete HSM, hardware TRNG, Biometric Enclave, TrustZone	Key extraction, side-channel, bootloader attacks
Layer 2 — Firmware	Verified U-Boot, custom AVB keys, ML bootloader integrity verification	Evil maid, firmware persistence (Vault 7 style), cold boot
Layer 3 — Hypervisor	KVM at EL2; pKVM memory isolation; VM domain separation	Cross-VM lateral movement, privilege escalation
Layer 4 — OS/Software	QWAMOS RASP, ML threat detection, nftables firewall, Tor routing	Zero-click exploits, network surveillance, data exfiltration

6.2 Hardware Kill Switches

Four recessed physical kill switches are located on the right spine of the device. These open physical electrical circuits — not GPIO lines controlled by software. No firmware, no OS, no hypervisor can restore connectivity once a kill switch is engaged.

Switch	Circuit Action
[1] NETWORK	Opens RF power supply circuit to cellular modem module. The modem loses power entirely — no 4G/5G/WiFi/Bluetooth transmission possible.
[2] MICROPHONE	Shorts microphone output lines to ground potential. No audio signal can propagate regardless of software state.
[3] CAMERA	Disconnects power rail to all camera modules. Sensor draws no power; no image capture possible.
[4] LOCATION	Disconnects power to GPS receiver and interrupts location data lines from cellular modem.

6.3 Emergency Protection Systems

System	Trigger & Mechanism
Panic Wipe	5-finger triple-tap gesture. Destroys all VM encryption keys via HSM key deletion command. UFS and NVMe AES keys overwritten with random data. Executed in <2 seconds.
Duress PIN	Alternate PIN boots convincing Android VM decoy profile. Primary VMs remain suspended in encrypted state, invisible to decoy environment.
Nuclear Tamper Wipe	HNCP/Tamper MCU detects tamper condition. Sends hardware signal to HSM — key material destroyed at silicon level before main SoC can boot. Operates with zero main battery level.
VM Snapshot Rollback	Any VM can be restored from encrypted snapshot after suspected compromise. Rollback command issued from Dom0.
Tor Kill Switch	If Gateway VM detects Tor circuit failure, nftables rules block ALL outbound traffic. No fallback to clearnet under any failure mode.

SECTION 7 — NETWORK & COMMUNICATIONS ARCHITECTURE

Isolated Modem — Mandatory Anonymization — PQC Transport

7.1 Cellular Modem — Isolated Domain

Module	Sierra Wireless EM9190 (or equivalent 5G Sub-6 + mmWave M.2 modem)
Standard	5G NR Sub-6 GHz + mmWave; 4G LTE fallback; 3G/2G legacy
Interface to RK3588	PCIe 3.0 x1 — routed through HNCP (Hardware Network Co-Processor)
Physical Isolation	Modem accessible ONLY via HNCP gating. No direct memory-mapped access from RK3588.
SIM	Dual: eSIM (primary) + physical nano-SIM (secondary) with hardware kill circuit
Vault 7 Mitigation	Baseband confined to Gateway VM. Gateway VM compromise does not yield modem persistence.

7.2 WiFi / Bluetooth / UWB

WiFi Standard	WiFi 7 (802.11be) — 2.4 GHz / 5 GHz / 6 GHz tri-band
WiFi Speed	Up to 5.8 Gbps theoretical (2×2 MIMO, 320 MHz channel, 4096-QAM)
Bluetooth	Bluetooth 5.4 — LE Audio, LC3 codec, direction finding
UWB	Ultra-Wideband (IEEE 802.15.4z) — secure ranging, device attestation
NFC	NFC Type A/B/F, ISO 14443, ISO 15693
Module Isolation	WiFi/BT/UWB module accessible via Gateway VM only — traffic mandatory through Tor/I2P stack.

7.3 Traffic Anonymization Stack

Layer	Technology	Function
Primary Anonymization	Tor (latest stable) — 3-hop onion routing	IP anonymization, traffic encryption, identity separation
Secondary Overlay	I2P — Invisible Internet Project	Alternative routing for I2P-native services and dead drops
DNS Protection	DNSCrypt — encrypted DNS resolution	Prevents DNS leakage; all resolution inside Gateway VM
DPI Defeat	WebTunnel transport — disguises Tor as HTTPS to CDN	Defeats deep packet inspection; traffic indistinguishable from standard HTTPS
Protocol Obfuscation	V2Ray — WebSocket, HTTP/2, gRPC, QUIC support	Multi-protocol fallback; circumvents protocol-level blocking
Bridge Protocols	obfs4, meek, Snowflake pluggable transports	Circumvents Tor-specific blocking by surveillance infrastructure
Behavioral Masking	ML-driven pattern obfuscation + Phantom Activity overlay	Defeats traffic analysis; real activity masked by synthetic decoy patterns
Kill Switch	Hardware + software dual kill switches	Zero clearnet fallback under any failure mode

SECTION 8 — PHYSICAL HARDWARE DESIGN

Chassis, PCB Stack, Connectivity & Form Factor

8.1 Form Factor

Form Factor	Candybar smartphone — single-piece aluminum alloy chassis
Display Size	6.9 inches (diagonal)
Target Dimensions	~163 × 78 × 9.2 mm (HWD) — subject to thermal and PCB stack validation
Target Weight	~245–265 g (battery + chassis + PCB stack)
Chassis Material	6000-series aluminum alloy — CNC-machined unibody; IP68 water/dust resistance
Rear Panel	Matte glass (Gorilla Glass 7i or equivalent) — conformal QD solar film laminated beneath
Finish Options	Matte Black (Tier 1); Titanium Gray (Tier 2/3 operational)
Spine — Right	4× recessed physical kill switches (Network, Microphone, Camera, Location)
Spine — Left	Volume up/down; SIM tray (nano-SIM + eSIM access)
Top Edge	USB-C 3.1 (power + data + DisplayPort Alt Mode); 3.5mm audio jack (optional)

8.2 PCB Layer Stack

PCB Layer	Components
Layer 1 — Top (Display Assembly)	Samsung LEAD 2.0 FMP OLED panel; under-display optical fingerprint sensor; ambient light / proximity sensor
Layer 2 — Upper Main Board	RK3588 SoC (PoP with LPDDR5X stack); UFS 4.0 1 TB storage; Infineon HSM; Hardware TRNG; Biometric Enclave IC; WiFi 7 / BT 5.4 / UWB module; NFC controller
Layer 3 — Network Enforcement	HNCP RISC-V MCU; Tamper Detection MCU; Sierra Wireless EM9190 5G modem; Kill switch relay array; Nuclear security rail power management
Layer 4 — Power / Storage	Custom graphene-silicon primary cell (pouch); BV100 nuclear cell (isolated ground plane); QD solar MPPT controller; USB-C PD 100W controller; NVMe SSD
Rear Panel Assembly	Perovskite QD conformal solar film; protective Gorilla Glass 7i overlay; antenna array (5G × 4, WiFi × 2, UWB × 1)

8.3 Camera System

Primary Camera	50 MP, f/1.7, OIS, PDAF — standard wide
Ultrawide Camera	50 MP, f/2.2, 120° FOV
Telephoto Camera	12 MP, f/2.8, 5× optical zoom, OIS
Front Camera	12 MP, f/2.2 — under-display or notch-free punch-hole
Privacy	Hardware kill switch cuts camera power rail completely.
Supplier	Sony Semiconductor (IMX series) or Samsung Semiconductor (ISOCELL) — per camera module

SECTION 9 — POST-QUANTUM CRYPTOGRAPHIC STACK

Full-Stack PQC — All Layers — No ECC Anywhere

Design Principle. VALKYRJA's cryptographic stack is designed around a single principle: no ECC anywhere in the security-critical path. ECDSA and X25519 are retained only as one component within hybrid constructions where classical algorithms are supplemented — never replaced — by post-quantum algorithms. Failure of all PQC algorithms simultaneously is required to compromise key material.

9.1 Key Encapsulation Mechanisms (KEMs)

Algorithm	Standard	Security Level	Role
ML-KEM-1024 (Kyber-1024)	NIST FIPS 203	Level 5 (AES-256 equivalent)	Primary KEM — all key exchanges
BIKE (Level 5)	NIST Round 4 Alternate	Level 5	Hybrid KEM component
HQC (Level 5)	NIST Round 4 Alternate	Level 5	Hybrid KEM component
Classic McEliece (Level 5)	NIST Round 4 Alternate	Level 5	Hybrid KEM component
X25519	RFC 7748	Classical 128-bit	Classical component in hybrid — not standalone
Hybrid Construction	Proprietary QWAMOS spec	Strongest of all components	KEM = ML-KEM XOR BIKE XOR HQC XOR McEliece XOR X25519

9.2 Digital Signature Schemes

Algorithm	Standard	Application
ML-DSA-87 (Dilithium)	NIST FIPS 204	Primary signing — hardware-backed in HSM; storage key signatures; firmware attestation
Falcon-1024	NIST FIPS 206	Compact signatures — certificate-constrained environments
SPHINCS+-SHA2-256	NIST FIPS 205	Stateless hash-based backup — immune to all algebraic attacks

9.3 Symmetric Primitives

Algorithm	Role	Quantum Status
ChaCha20-Poly1305	Authenticated encryption (AEAD) — all transport and storage encryption	Classical-secure (256-bit key)
BLAKE3	Hashing — integrity verification, key derivation input	Quantum-resistant at 256-bit output
Argon2id	Key derivation — GPU/ASIC-resistant KDF from passphrase	Memory-hard; resistant to dedicated hardware attacks
HKDF-BLAKE2b	Key expansion — derives per-purpose keys from master key material	Classical-secure; quantum-safe at 256-bit output

SECTION 10 — QWAMOS SOFTWARE SPECIFICATION

Operating System — v3.1.0 — 27/27 Phases Complete

10.1 Overview

Full Name	Qubes+Whonix Advanced Mobile Operating System
Version	3.1.0 (January 2026) — v3.2.0 targeted for device launch
License	AGPL-3.0 (open-source, copyleft — all derivatives must be open-source)
Repository	github.com/Dezirae-Stark/QWAMOS
Development Phases	27 / 27 complete (100%)
Codebase Size	50,000+ lines of code
Primary Languages	Python 3.9+, Dart/Flutter, TypeScript, Java/Kotlin
Architecture	ARM64-native KVM hypervisor OS with Qubes-style VM compartmentalization
Build System	Reproducible builds (repro-build.sh); SLSA Level 3 provenance; GPG-signed releases

10.2 Virtual Machine Domain Architecture

VM Domain	Network Access	Base OS	Purpose
Dom0 / Control VM	None	Minimal Linux	VM lifecycle, security policies, ML threat detection — privileged, no network
Gateway VM	Direct (filtered)	Whonix-style Linux	Tor/I2P/VPN/DNSCrypt routing — all user VMs route through here
Android VM	Via Gateway	AOSP Android 14+	Primary daily use environment — consumer app ecosystem
Arch Linux VM	Via Gateway	Arch Linux	Secure comms — Signal, ZRTP, steganography, PQC operations
Kali NetHunter VM	Via Gateway	Kali Linux	Offensive security, penetration testing toolkit
Ubuntu Dev VM	Via Gateway	Ubuntu 24.04 LTS	Development environment, AI App Builder pipeline
Vault VM	None (air-gapped)	Minimal Linux	Key storage, classified material, cryptographic operations
Disposable VM	Via Gateway	Ephemeral Debian	One-time-use — fresh per session, automatic wipe on close

10.3 User Experience — Profile Abstraction Layer

Profile	VM Configuration	FMP State
Everyday	Android VM active; Gateway VM routing; standard Tor circuit	Off
Private	Fresh isolated Android VM; separate Tor identity; no cross-VM data	Standard Privacy
Secure	Arch Linux VM; PQC comms; ZRTP voice; full E2E stack	Maximum Privacy

Profile	VM Configuration	FMP State
Ghost	Fresh Disposable VM; WebTunnel DPI defeat; Phantom Activity overlay	Maximum Privacy

10.4 AI & Machine Learning Stack

Component	Technology	Function
On-device LLM (Kali GPT)	Local inference via RK3588 NPU (6 TOPS)	Security analysis, threat assessment, exploit evaluation
External AI (Claude)	API via Tor (isolated channel)	Architecture design, code review, compliance guidance
External AI (ChatGPT)	API via Tor (isolated channel)	Code quality, UI/UX assistance, test generation
Consensus Engine	ai_security/orchestrator.py	Adjudicates conflicts between AI models; majority-rule synthesis
Threat Detection — Autoencoder	Unsupervised neural network (Dom0)	Novel/zero-day behavioral anomaly detection
Threat Detection — Random Forest	Supervised ensemble (Dom0)	Known attack signature and pattern matching
Threat Detection — LSTM	Recurrent neural network (Dom0)	Temporal sequence attack detection across time windows
AI Governor	hypervisor/ai_governor.py	ML-driven CPU/memory/I/O resource allocation per VM
LoRA Fine-tuning	ai_security/lora_finetuning.py	On-device model fine-tuning for threat intelligence adaptation

10.5 SecureType Keyboard

Feature	Implementation
Per-Keystroke PQC Encryption	ML-KEM-1024 encryption applied to each individual keypress before leaving keyboard subsystem
Coordinate Obfuscation	±5 px random noise added to touch coordinates — defeats stylometric fingerprinting
Layout Randomization	Keyboard layout reshuffled every 30 seconds — defeats layout memorization shoulder surfing
Anti-Screenshot	FLAG_SECURE active whenever keyboard is visible — no screen capture possible
Clipboard Isolation	Clipboard contents encrypted and scoped per-VM — no cross-VM clipboard access
AI Typing Verification	Behavioral biometric model detects typing rhythm anomalies — alerts on unauthorized user

SECTION 11 — SUPPLIER PROCUREMENT TARGETS

Component Sourcing Strategy & Primary Contacts

11.1 Critical Path Components

Component	Target Supplier(s)	Priority	Lead Time Est.
RK3588 SoC	Rockchip Electronics (direct); Arrow, Avnet, Mouser	P0 — Critical	8–16 weeks (stock); 16–24 weeks (custom)
Samsung FMP LEAD 2.0 Display	Samsung Display Corporation — Mobile Display Business Division (B2B direct)	P0 — Critical	12–18 months (custom panel program)
32 GB LPDDR5X RAM	Samsung Semiconductor; SK Hynix; Micron Technology	P0 — Critical	12–16 weeks
1 TB UFS 4.0 Storage	Samsung Semiconductor (KLUDG8); SK Hynix (H28U1); Micron (MTFC)	P0 — Critical	12–16 weeks
Graphene-Silicon Primary Cell	Lyten Inc. (US); Graphene Manufacturing Group (AU); Sila Nanotechnologies	P0 — Critical	18–24 months (custom cell program)
Betavolt BV100 Nuclear Cell	Betavolt New Energy Technology Co. (Beijing) — NRC licensing parallel track	P0 — Critical	12–18 months + regulatory
Infineon HSM (SLB9672)	Infineon Technologies AG; Digi-Key, Mouser	P1 — High	16–20 weeks
Sierra Wireless EM9190 5G Modem	Semtech Corporation (Sierra Wireless parent); Arrow Electronics	P1 — High	12–16 weeks
Perovskite QD Solar Film	Saule Technologies (PL); Quantum Solutions; Greatcell Solar	P1 — High	18–24 months (custom deposition)
WiFi 7 / BT 5.4 / UWB Module	Qualcomm FastConnect 7900; MediaTek Filogic 880; NXP SR150	P2 — Standard	12–16 weeks
Camera Modules	Sony Semiconductor (IMX989/IMX766); Samsung ISOCELL (HP9/GN5)	P2 — Standard	16–20 weeks
NVMe SSD (512 GB)	Samsung (PM9A3); SK Hynix (PC801); Western Digital (SN850X custom)	P2 — Standard	12–16 weeks

11.2 Manufacturing Engagement Strategy

ODM Partner	Profile	Engagement Priority
Foxconn Technology Group	World's largest contract electronics manufacturer; significant security device experience; US and Taiwan facilities	Primary
Pegatron Corporation	Apple ODM partner; high-quality assembly; significant security practices; Taiwan and Mexico facilities	Primary
Compal Electronics	Established security device experience; PCB integration capabilities; Taiwan	Secondary
Flextronics (Flex Ltd.)	US manufacturing facilities; security clearance-adjacent capability; ITAR experience	Secondary (Tier 3 option)
Benchmark Electronics	US domestic manufacturing; specialized high-reliability electronics; suited for Tier 3 operational variant	Tier 3 Dedicated

SECTION 12 — REGULATORY & COMPLIANCE FRAMEWORK

Certification Requirements & Jurisdiction Considerations

12.1 Required Certifications — All Tiers

Certification	Requirement
FCC Part 15 (US)	Required for all RF-emitting devices sold in US market. Covers 5G modem, WiFi 7, Bluetooth, UWB, NFC.
CE Mark (EU)	Required for EU market. Covers Radio Equipment Directive (RED), EMC Directive, RoHS.
PTCRB / GCF	Carrier certification for 5G/4G cellular bands. PTCRB for North America; GCF for international carriers.
IC (Industry Canada)	Required for Canadian market.
IEC 62133 / UN 38.3	Lithium battery safety. Required for all custom graphene-silicon cell configurations.
RoHS 3 Compliance	Restriction of Hazardous Substances — affects component material selection across all PCBs.
Bluetooth SIG Qualification	Required for use of Bluetooth trademark and royalty-free coexistence stack.
Wi-Fi Alliance Certification	Required for Wi-Fi 7 (802.11be) trademark use and interoperability certification.

12.2 Nuclear Cell — Regulatory Considerations

Incorporation of Nickel-63 (Ni-63) radioactive isotope in the BV100 nuclear security cell requires engagement with the Nuclear Regulatory Commission (NRC) in the United States, or the national regulatory equivalent in the manufacturing jurisdiction.

- NRC License: Specific or general license for possession of byproduct material (10 CFR Part 30)
- BV100 contains approximately 20 curies Ni-63 per cell — above general license threshold
- Shipping: IATA Dangerous Goods Regulations (DGR) Section 10 — radioactive material; special packaging required
- End-of-life: Ni-63 decays to stable Cu-63 — no special disposal required at product end-of-life

RECOMMENDATION: Engage NRC pre-application consultation concurrent with Betavolt procurement discussions.

12.3 Export Control

Framework	Applicability
EAR (Export Administration Regulations)	Post-quantum cryptography may be subject to EAR controls under ECCN 5E002. Legal review required for Tier 3 operational export.
ITAR (International Traffic in Arms Regulations)	Tier 3 Operational variant may trigger ITAR if device is classified as 'defense article.' Legal review required before Tier 3 specification is finalized for export.
Wassenaar Arrangement	Multi-lateral export control framework for dual-use technologies. Post-quantum cryptographic components require review in each export destination jurisdiction.

APPENDIX A — BILL OF MATERIALS SUMMARY

High-Level Component BOM for Procurement Planning

Unit costs are indicative estimates for small-volume (1,000–10,000 unit) production, subject to supplier negotiation, volume discounts, and market conditions. Costs in USD.

Component	Supplier Target	Est. Unit Cost (Small Vol.)	Notes
RK3588 SoC	Rockchip / Arrow / Avnet	$35–55	Volume pricing at 10k+ units significantly lower
32 GB LPDDR5X RAM	Samsung / SK Hynix	$45–65	PoP integration adds $5–10 for packaging
1 TB UFS 4.0 Storage	Samsung / SK Hynix	$40–60	
512 GB NVMe SSD	Samsung / SK Hynix / WD	$25–40	Custom M.2 form factor adds tooling cost
Samsung FMP LEAD 2.0 Display	Samsung Display Corp.	$80–130	Custom panel; pricing TBD via direct B2B; MOQ critical
Graphene-Silicon Primary Cell	Lyten / GMG / Sila	$60–120	Custom cell; early-stage supplier; high uncertainty
Betavolt BV100 Nuclear Cell	Betavolt (Beijing)	$200–500	Highly uncertain; regulatory cost overhead not included
Perovskite QD Solar Film	Saule / Quantum Solutions	$30–60	Custom conformal deposition; area-dependent
Infineon HSM (SLB9)	Infineon / Digi-Key	$8–15	
Sierra Wireless EM9190 5G	Semtech / Arrow	$45–75	Includes carrier certification cost amortization
WiFi 7 / BT / UWB Module	Qualcomm / MediaTek	$12–20	
Camera Modules (3×)	Sony / Samsung ISOCELL	$25–45	Per camera module; 3 required
Biometric Enclave + Sensor	Synaptics / Goodix	$15–25	
Hardware TRNG (v1)	Maxim / STM / Microchip	$3–6	Classical ring oscillator + shot noise — v1 baseline
Glass Photonic QRNG (v2)	Corning EAGLE XG glass + femtosecond laser system (capital equipment); photonics lab engagement for FLDW process development	$15–40	v2 integration — no cleanroom required. Chip-scale unit cost after process development. NRE: $5–15M for miniaturization engineering.
PCB (multilayer custom)	TTM / Tripod / Shennan	$15–30	6–8 layer custom stack
Chassis + Mechanical	Foxconn / Pegatron tooling	$25–50	Includes CNC aluminum unibody amortization
Miscellaneous passives / connectors	Various	$8–15	
ESTIMATED TOTAL BOM	—	$690–1,349	Excluding: regulatory, certification, software, tooling amortization

Cost Reduction Trajectory: BOM cost at small volumes is elevated by custom component premiums, particularly the graphene-silicon cell, nuclear security cell, and FMP display panel. At 100,000+ unit scale, BOM cost is expected to fall to the $350–550 range. Tier 1 consumer device at high volume funds the cost structure for Tier 2/3 premium variants.

APPENDIX B — QWAMOS DEVELOPMENT PHASE COMPLETION

All 27 Phases Complete — v3.1.0 (January 2026)

Phase	Name	Status	Key Deliverables
1	Core Hypervisor	✓ Complete	ARM64 KVM hypervisor, VM lifecycle management
2	Network Isolation	✓ Complete	Whonix-style gateway, Tor/I2P routing
3	Storage Encryption	✓ Complete	Per-VM encrypted volumes, key management
4	Post-Quantum Crypto	✓ Complete	ML-KEM-1024, ChaCha20-Poly1305, BLAKE3, Argon2id
5	Firewall & Policies	✓ Complete	Per-VM firewalls, 12 policy toggles, panic wipe
6	AI Integration	✓ Complete	Triple-AI coordination — Kali GPT, Claude, ChatGPT
7	ML Threat Detection	✓ Complete	Autoencoder, Random Forest, LSTM detection models
8	SecureType Keyboard	✓ Complete	Per-keystroke PQC, coordinate obfuscation, layout shuffle
9	AI App Builder	✓ Complete	Triple-AI code generation, automated security audit
10	Hardware Security	✓ Complete	ML bootloader lock, Vault 7 mitigation
11	Flutter UI System	✓ Complete	26 custom widgets, GLSL shaders, Material Design 3
12	KVM Acceleration	✓ Complete	VirtIO drivers, hardware virtualization optimization
13	PQC Storage	✓ Complete	ML-DSA-87 hardware-backed keys, StrongBox integration
14	GPU Isolation	✓ Complete	Per-VM GPU slices, Vulkan passthrough
15	AI Governor	✓ Complete	ML resource allocation, predictive VM scaling
16	Cluster Mode	✓ Complete	Multi-device mesh, live VM migration across devices
17	HSM Integration	✓ Complete	TPM 2.0, FIDO2, TrustZone integration
18	Network Privacy (Enhanced)	✓ Complete	WebTunnel, V2Ray, behavioral obfuscation (v3.1.0)
19	Offensive Security	✓ Complete	Vulnerability scanner, penetration testing toolkit
20	Enhanced AI/LLM	✓ Complete	Multi-model orchestration, LoRA fine-tuning
21	App Security	✓ Complete	RASP, package verification, auditing
22	Secure Comms	✓ Complete	Signal Protocol, ZRTP, steganography
23	Forensics	✓ Complete	Memory forensics, chain of custody
24	Compliance	✓ Complete	CIS, NIST 800-53, OWASP, Common Criteria
25	UX / Accessibility	✓ Complete	React Native UI, voice control, gesture navigation
26	IoT Ecosystem	✓ Complete	Device discovery, MQTT/Zigbee/Z-Wave, wearables
27	Quantum Resistance	✓ Complete	BIKE, HQC, McEliece, QKD simulation, hybrid crypto

APPENDIX C — COMPETITIVE SECURITY ARCHITECTURE COMPARISON

VALKYRJA vs. Current Market Landscape

Capability	VALKYRJA	S26 Ultra	Pixel 10 Pro	Librem 5	Bittium Tough
KVM / Type-1 Hypervisor	Yes — native	No	Partial (AVF)	Yes (slow)	No
VM Domain Isolation	8 domains	None	1 (Microdroid)	Yes	No
RAM	32 GB	12–16 GB	16 GB	4 GB	4 GB
Post-Quantum Crypto	Yes — full stack	No	Partial	No	Partial
Mandatory Tor for all traffic	Yes	No	No	No	No
Hardware Kill Switches	4× relay	None	None	3× switch	1× (network)
Discrete HSM	Yes (Infineon)	TrustZone	Titan M2	No	Yes
Privacy Display (FMP)	Yes + FLAG_SECURE	FMP only	None	None	None
Nuclear Security Rail	Yes (BV100)	None	None	None	None
Solar Harvesting	Yes (QD perovskite)	None	None	None	None
6-Minute Charge	Yes (graphene-silicon)	No (~80 min)	No (~70 min)	No	No
Anti-Surveillance (ultrasonic)	Yes	No	No	No	No
Behavioral Obfuscation (ML)	Yes	No	No	No	No
Per-Keystroke PQC Encryption	Yes (SecureType)	No	No	No	No
Open Source OS	Yes (AGPL-3.0)	No	Partial	Yes	No

Obsidian Circuit
Technical Product Memorandum — Onyx | Codename: VALKYRJA
PROPRIETARY & CONFIDENTIAL — All Rights Reserved — April 2026
Prepared by Desirae Stark, Chief Architect
QWAMOS v3.1.0 — github.com/Dezirae-Stark/QWAMOS