COMMERCIAL PRIVACY-SECURE MOBILE OPERATING SYSTEM

BharatDroid Vault

Sovereign control of the mobile software boundary, tested on commercial off-the-shelf hardware

8h 01m	0 bytes	23 / 23	< 648 ms	0 / 384k
locked-idle observation	measured idle IP increase	launcher apps opened	sampled radio cut-off	non-zero mic bytes

01	**Sovereign build and signing**	Android-derived OS integrated with Vault and signed with founder-controlled release and Android Verified Boot keys. The bake path can be adapted to supplied COTS device trees without depending on foreign-held OS signing keys.
02	**Google-free system base**	The tested image contains no GMS, GSF or Play Services packages. Operator-controlled application distribution remains distinct from user-initiated access to a third-party store.
03	**Enforced integrity**	Runtime checks reported Verified Boot green, dm-verity enforcing, SELinux enforcing, release-keys, read-only system partitions, no development overlay and no su binary.
04	**Vault control plane**	App identity mediation, scoped identifiers, non-exportable key brokering, sensor starvation, foreground-only egress, fail-closed VPN and operator-selected WireGuard upstream are governed as one device policy.
05	**Measured working prototype**	Zero additional Wi-Fi or mobile IP bytes were measured over an eight-hour locked interval. Active app traffic entered tun0; ordinary probes received no physical markers or useful sensor data; lock removed the tested underlays.

Commercial position: licensable secure-OS integration, COTS device adaptation, signed updates and operator policy. Current status: working handset prototype; independent certification, repeatable multi-model builds and supply qualification remain future gates.

GOVERNMENT-DECLARED MOBILE SECURITY REQUIREMENTS

From published challenge to tested device controls

The comparison is capability-specific. It does not claim that one platform is universally superior, and it separates prototype evidence from certification.

Open challenge / incident	How Vault responds	How alternatives address it	Mapped evidence
Unauthorized app collection and transfer. MeitY described apps collecting and transmitting user data to servers outside India as a threat to state security. [S02]	Default-deny application policy; identity markers are denied, scoped or masked; tracker DNS is dead-ended; application egress is admitted only through the Vault boundary.	Stock Android, iOS and enterprise MDM provide permissions, app vetting and VPN controls. GrapheneOS adds a network permission. Vault differentiates through measured marker substitution plus foreground-only tunnel admission.	E02, E03, E04, E05 IMEI null; Wi-Fi identity masked; raw bypass and underlay binding blocked; active flows recorded through tun0.
Smartphone security across service devices. iDEX DISC 9 called for a smartphone security solution able to detect malicious calls/IPs and protect service-personnel data across smart devices. [S01]	COTS-oriented build integration, operator signing, policy-controlled apps, protected network path, local evidence collection and a path to controlled signed updates.	BharOS also presents a COTS, no-default-app and private-app-store model. Knox is tied to Samsung hardware. GrapheneOS officially supports a narrow device family. Vault is designed as an adaptation layer for supplied device trees.	E01, E07, E08 Working Nothing Phone (1); release-signed immutable system; no GMS packages; 23 launcher apps completed the test pass.
Protected data in transit over untrusted networks. NSA CSfC mobile guidance uses independent layered commercial components and two nested tunnels for protected mobile access. [S05]	Vault governs downstream application UIDs and exposes only tun0 to apps; the operator selects the upstream WireGuard configuration. Lockdown stays enabled and physical underlay binding is denied.	CSfC is a reference architecture requiring evaluated components and registration. Enterprise always-on VPN protects transit but normally does not combine identity, sensor and key mediation. Vault is not represented as CSfC-certified.	E02, E03, E07 VPN exit visible to probes; raw TCP/UDP and physical-network binding failed; lock retained tun0 with no usable underlay.
Assurance and acquisition confidence. STQC's IC3S evaluates IT security products and Protection Profiles under Common Criteria. [S07]	Owner-held release/AVB keys, Verified Boot, dm-verity and SELinux establish an inspectable trust baseline for later product evaluation and device-specific certification.	Knox offers mature hardware-rooted attestation; Apple tightly integrates hardware and OS; GrapheneOS uses verified boot on supported Pixels. Vault's differentiator is sovereign policy ownership and COTS adaptation, not completed certification.	E01, E07 Runtime: green verified boot, verity enforcing, SELinux enforcing, locked flag, release keys, no overlayfs and no su.

Source IDs resolve in the glossary. Competition descriptions use each platform's own published documentation; they are not laboratory comparisons.

OPERATIONAL INCIDENTS AND ATTACK PATHS

Controls that go beyond an app blocklist

Vault is designed to reduce the useful data available to an installed application, not merely to tell personnel which applications to avoid.

Open challenge / incident	How Vault responds	How alternatives address it	Mapped evidence
Honey-trapping and social engineering. India's Ministry of Defence has recorded honey-trapping cases and issued advisories to service personnel. [S03]	A newly installed app remains an ordinary UID. It receives masked or null identifiers, controlled foreground egress and no useful background sensor feed; lock cuts the tested underlays.	Training, advisories, allowlists and MDM can prevent or remove risky apps. Vault adds containment when a permitted or deceptive app is present, while preserving the need for operational discipline.	E02-E06 Role elevation did not reveal telephony identifiers; foreground tunnel grants were revoked on close; sensors delivered no data.
Location and pattern-of-life exposure. The U.S. Army reported that Strava heat maps could reveal bases and support targeting of individuals. [S04]	Location returned null; motion and all enumerated sensor classes delivered zero samples; Wi-Fi scan returned no results; SSID/BSSID/MAC were withheld or masked.	Standard permission prompts depend on user choice. GrapheneOS adds sensor and network toggles. Vault's tested policy makes no useful sensor delivery the default for ordinary probes and ties lock state to radio cut-off.	E04, E05, E06 38 sensor classes enumerated, zero registered/delivering; location null; role app saw masked Wi-Fi identity.
Targeted spyware and exploit-driven collection. Apple's Lockdown Mode limits features for people facing sophisticated mercenary spyware. [S09]	Vault reduces post-compromise value by starving app-facing sensors, separating keys, denying physical-network selection and enforcing a Google-free, signed system boundary.	Apple Lockdown Mode and GrapheneOS provide substantial exploit-surface reduction. Vault does not claim exploit immunity; its distinct focus is sovereign policy mediation and measured data minimization across identity, network, sensors and keys.	E01, E04-E07 No useful sensor/media output, non-exportable key, cross-UID decrypt rejected, direct network bypass blocked.
Locked handset background activity. Conventional mobile platforms preserve connectivity for notifications and services, leaving policy dependent on application behavior.	Lock transition disables tested Wi-Fi, Bluetooth and mobile-data settings while VPN lockdown remains active. With no underlay, scheduled WireGuard retries fail locally rather than bypassing Vault.	Airplane mode can suppress links but is manual and coarse. MDM can enforce settings. Vault makes the screen-lock transition part of the OS privacy policy and was measured in the working prototype.	E02, E09 Wi-Fi observed off by the 648 ms sample; Bluetooth/mobile data off; zero measured Wi-Fi or mobile IP-byte increase across 8h01m.
Hardware key reuse and cross-app extraction.	Vault exposes a mediated keystore path, produces non-exportable keys and rejects cross-UID decryption. Hardware-attestation key requests from the probe were refused.	Knox Vault offers a dedicated hardware subsystem and mature attestation. Vault's differentiator is operator-owned brokering policy across adapted COTS builds; hardware assurance still depends on the selected device and certification.	E04 Standard Keystore2 hidden from ordinary app; Vault service visible; encoded key null; cross-UID decrypt rejected.

Bounded conclusion: the evidence supports zero measured idle IP telemetry egress in the observed window and controlled, tunnelled foreground traffic. It does not establish immunity to every exploit, RF emissions, baseband behavior or future software state.

REPLACEMENT-PRODUCTION ECONOMICS

What it would cost to recreate and productize the present capability

This is a transparent 24-month engineering replacement-cost model, not a valuation, funding commitment or fleet manufacturing budget.

Workstream	Illustrative basis	INR crore
Kernel and HAL engineering	Two senior engineers for 24 months, including BSP adaptation, suspend/wake behavior and vendor interface reconciliation.	**2.88**
Framework, network and security	Two senior engineers for 24 months covering framework mediation, VPN, WireGuard, identity policy, SELinux and updates.	**2.40**
QA, probes and regression	Two engineers for 24 months covering app compatibility, adversarial probes, battery, lock-state and multi-model regression.	**1.44**
Release, DevSecOps and reproducibility	One release/security lead for 24 months covering signing, OTA, recovery, dual-slot, provenance and build automation.	**0.96**
Specialist BSP and crypto contracts	Device-specific modem, Wi-Fi, Bluetooth, camera/audio, cryptography and certification preparation.	**1.60**
Secure lab, build rigs and devices	Compilation servers, storage, representative handsets, network instruments and controlled test infrastructure.	**0.70**
Independent assessment and certification	Red team, Common Criteria/STQC preparation, external labs, documentation and retest reserve.	**1.50**
Programme, legal and supply readiness	Technical programme management, IP/legal work, procurement documentation and COTS supply-chain qualification.	**0.82**
Illustrative 24-month total	**Range sensitivity should be applied for hiring market, number of supported device families and certification scope.**	**12.30**

The model excludes handset bill of materials, fleet volume, classified-network accreditation and production support at scale. Those are deployment economics, not reconstruction cost.

MARKET OUTLOOK

A sovereign secure-mobile category, not a consumer ROM market

The commercial opportunity is the repeated engineering, certification and lifecycle work required to put controlled mobile computing on approved COTS fleets.

INDIA: DECLARED NEED	GLOBAL: COTS SECURITY MODEL	COMMERCIAL ROUTES
iDEX has published a smartphone-security challenge for service personnel, while MeitY actions document unauthorized mobile-data transfer as a national-security concern. BharOS independently validates demand for an indigenous COTS mobile OS and private app delivery.	NSA CSfC demonstrates an established government pattern: layered, evaluated commercial components configured for secure mobile access. BharatDroid targets the engineering layer below fleet operations - the device OS, policy and sovereign signing path - while future certification remains mandatory.	Potential revenue lines are device adaptation and non-recurring engineering, per-device provisioning, annual signed update and policy support, on-premise fleet tooling, certification services, and licensing to OEM, DPSU, paramilitary, diplomatic and critical-infrastructure programmes.

Commercial delivery model

01	**Device adaptation and NRE**	Port and qualify the signed Vault image, vendor interfaces and policies for each selected COTS model.
02	**Provisioning and signed lifecycle**	Per-device enrollment, fleet policy, signed OTA, rollback, evidence capture and annual security maintenance.
03	**Certification and deployment services**	Threat model, test artefacts, STQC/Common Criteria preparation, red-team closure and controlled pilot support.
04	**OEM, DPSU and integrator licensing**	License the OS policy, bake system and update authority into approved domestic supply and managed-service programmes.

No revenue, customer-count or procurement-volume claim is made here. Market entry depends on independently verified security, device supply, certification and a sponsored field pilot.

EVIDENCE GLOSSARY

Fresh device evidence captured 3 October 2026

Each evidence file is retained locally with a SHA-256 digest. Short hashes below are prefixes of the complete digest and support chain-of-custody review.

ID	Evidence	What it establishes	SHA-256 prefix
E01	02-build-root-immutability.txt	BharatDroid 17 Closure; slot B; release-keys; locked runtime flag; green Verified Boot; verity and SELinux enforcing; read-only dm/erofs system mounts; no overlay or su.	4D5DA3A0B4224248
E02	final-lock-transition/01-transition-samples.txt and 02-locked-after-120s.txt	Lock-state convergence; Wi-Fi off by sampled 648 ms point; Bluetooth/mobile data off; lockdown VPN retained; physical interfaces down or without routed application underlay.	B00F5C33C3E12D71 / 7C63AC4E30268BFF
E03	active-app-pass/92-appwise-vpn-deltas.csv plus per-app logs	All 23 launcher apps started; measured foreground traffic entered the Vault VPN; Instagram and Aurora created the largest short-window tun0 deltas; cellular counters did not change across the pass.	F05C75732BAA01A5
E04	10-probe-a-log.txt and 12-probe-b-log.txt	Ordinary-app identity, keystore, sensor, scan, DNS and network-bypass tests; cross-UID key rejection; VPN exit exposure rather than access-link IP.	6D7941D51B594A49 / 08683C8DE129EBEF
E05	role-identifier-probe/11-role-probe-log.txt	Temporary Dialer/SMS role assignment still returned null telephony identifiers, decoy operator values and masked Wi-Fi identity. Original roles were restored.	B06B082BA7137BA9
E06	offline-audio-probe/06-probe-log.txt and capture.pcm	RECORD_AUDIO granted; AudioRecord entered recording state; 384,000 PCM bytes read with zero non-zero bytes; no useful microphone signal returned.	29593793EB5B997D
E07	red-probe 19-post-vpn-security.txt; final-lock 04-final-integrity-cleanup.txt	Post-test VPN/security posture and final cleanup: enforcement retained and disposable probes removed.	Bundle manifests retained
E08	03-google-vault-packages-services.txt	No GMS, GSF or Play Services packages present; Vault components enumerated.	01FBC74C559177D5
E09	51-idle-window-logcat-epoch.txt and 14-netstats.txt	Exact 8h01m locked window; retained mobile and Wi-Fi sample values remained unchanged; blocked Qualcomm time-assistance DNS retries were visible without successful egress.	51274030A7ADD78C / 03C7FE7EB3521F9E

Measured conclusion

The fresh run supports zero measured idle IP telemetry egress during the observed locked interval, controlled foreground-only app egress through Vault/tun0, identity and key mediation, sensor starvation, and fail-closed lock behavior. It does not establish RF silence, baseband protocol silence, exploit immunity or completed government certification.

SOURCE GLOSSARY

Primary public references behind the challenge and comparison

Public sources establish the operational need and describe alternative capabilities. BharatDroid performance claims come from the retained device evidence on the previous page.

ID	Reference	Public URL
S01	iDEX DISC 9 - Development of a Smartphone Security Solution / Application	Open official source
S02	Press Information Bureau - Government blocks 118 mobile apps over unauthorized collection and transmission of data	Open official source
S03	Press Information Bureau, Ministry of Defence - Honey-Trapping in Armed Forces	Open official source
S04	United States Army - DoD looking into the impact of fitness trackers on soldier safety	Open official source
S05	NSA Commercial Solutions for Classified - Mobile Access Capability Package and FAQ	Open official source
S06	NSA - Mobile Device Best Practices	Open official source
S07	STQC - Indian Common Criteria Certification Scheme	Open official source
S08	GrapheneOS - Features overview	Open official source
S09	Apple Platform Security - Lockdown Mode security	Open official source
S10	Samsung Knox - Hardware-backed security	Open official source
S11	IIT Madras - Indigenous BharOS for commercial off-the-shelf handsets	Open official source

WHAT IS PROVEN	WHAT REMAINS TO BE PROVEN
A working device image with sovereign software signing, Google-free system packages, enforced runtime integrity, Vault-mediated application identities and keys, controlled app egress, sensor starvation and zero measured idle IP traffic in the observed interval.	Independent source review and red-team certification; device-family reproducibility; fastboot/owner-key chain reconciliation on every production model; Common Criteria or applicable government certification; supply-chain qualification; production update SLAs; RF and baseband laboratory characterization.

Prepared as an investor diligence brief. Security evidence is device- and time-bounded; commercial cost assumptions are illustrative and should be re-baselined against hiring, certification and target-hardware scope before investment decisions.