BLK-1 encrypted blackOS secure communication system

Locatie **Noord-Holland, Amsterdam**
https://www.advertentiex.nl/x-2029813-z

Authorised distributor for Benelux
Available to legal entities
For inquiries, contact us via Marktplaats or at +31610078382 (WhatsApp or Signal)

BLK-1. Secure communication system.

Anonymous communication over Tor hidden servicesBaseline AOSP multi-layered securityReduced attack surfaceLimited app inclusionMinimal kernelNon-integrated GMS or telemetryCovert design blackOS.
Custom operating system, based on the Android™ Open Source Project, tailored for hostile environments.

Covert.
Covert design until unlocked, blending within millions of other mobile devices.

Features.
Standard Android-based device with the 6+" screen, nano-SIM, fingerprint (under display, optical), IP68 dust/water resistantBased of the AOSP multi-layered security (verified boot, application sandbox, exploit mitigations, runtime permissions model)Includes built-in support for PPTP, L2TP/IPSec, and WireGuard® (externally provided as is) VPN clientsSupport for disabling internet automatic time (connecting and exposing IP address)Seamless automatic security and feature updatesEnd-to-end encrypted messagesTwo-way (1:1) communicationPreventing group compromiseRelayed and encrypted in transit over the Tor network anonymizing originsP2P (peer-to-peer), direct device connections without the central serverAutomatic lockdown on inactivityAlways-on user-configurable auto-deletion of messagesIn-app camera support capturing still images, EXIF metadata strippedOn-device creation, storage, and management of identity, contacts, and messagesHardening against remote exploitation by disabling (stop scanning or connecting to) 3G and 5G networks (with 2G always disabled)Cellular connectivity security mitigations by not integrating traditional voice calls or SMS, MMS, emergency-related services and moreSecurity-focused memory allocator providing hardening against the most common vulnerabilitiesOffline keyboard without permissionsDestructive or nondestructive emergency actions can be triggered manually, or automatically by incorrect password attempts or disruptive SIM card state changesProtection of database cryptographic key within hardware security module (HSM)Locally applied

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

BLK-1 encrypted blackOS secure communication system https://www.advertentiex.nl/x-2029813-z

restricted device and user policies. No out-of-device remote managementSoftware-based self-destruct mechanism if the device is not unlocked within a specified timeframeUSB connection and data transfer fully disabled, used only for chargingFurther reduced USB attack surface complexity by controlling charging permissionsReduced local and remote attack surface by removing unused features, not limited to Wi-Fi®, NFC, Bluetooth®, USB, Ultra-wideband, GNSS, cellular services IMS and Telecom, Audio, Sound, development tools ADB and Fastboot, Tethering, PeripheralsCompartmentation using a second password, different cryptographic keys , the utilization of a sandbox environmentDetection and lockdown on negative environment motion (forced acceleration or in close proximity of the device)Use your own SIM cardNon-integrated Google Mobile Services (GMS), or telemetryDetailed battery stats with near real-time data collection, monitoring and reporting all services and apps on the device and their power and battery impactOn-premises servers for over-the-air (OTA) updates, NTP for obtaining accurate time, further minimizing unique network footprintOptional biometric unlock for critical apps, additionally protecting existing settingsCustom NTP server option for obtaining accurate timeRemote erase by trusted contacts in case of emergencyAbility to set a duress password for erasing the