Technical Specifications

RENATI

DEVICE & OPERATING SYSTEM

PROPRIETARY SECURITY

- Proprietary Renati Mobile Device Management (RMDM)
- Custom Secure Socket Tunnel replacing Google's Firebase Cloud Messaging (FCM). Enables real-time bi-directional communication & extends battery life
- Secure mobile operating system (OS) with remote management capabilities
- Custom fork of the Android Open Source Project (AOSP)
- Source code available for review & auditing
- Custom hardened Linux kernel using control flow integrity & Kernel Self Protection Project
- Security enhanced custom keyboard
- Custom designed over the air (OTA) update server that implements A/B updates
- Unique signing key prevents OS from being replaced/modified via unauthorized updates
- Optimized for select Pixel device models

SECURITY ENHANCEMENTS

- Zero trust authentication
- Quality & technical controls
- Application sandbox
- Dedicated secure subsystem
- Android Verified Boot (AVB)
- Duress password on lockscreen
- Latest Android security updates
- Self destruct bootloader tamper protection

DEVICE HARDENING

- Removed location tagging, tracking & identifiers (GPS, hotspot, emergency services, fused location)
- Google-free Android device, no third-party apps or services
- Disabled Bluetooth, NFC & NDEF Push
- No internet browsing
- No clipboard, USB data or USB signalling
- No reliance on syncing with servers
- Removed screen capture capabilities

SERVER-SIDE SECURITY

- Canadian owned & operated with pro-encryption & privacy laws
- Valid trust anchor certificate
- Reliability
  - 99.99% up time
  - High availability disaster recovery
- Private data center
  - Ballistic physical protection, 24/7 surveillance
  - Secure against remote, Distributed Denial of Service (DDoS) & Man in the Middle (MitM) attacks
  - Custom designed microservice infrastructure utilizing RabbitMQ, under 200 millisecond message speed

CUSTOM SOFTWARE

CHATMAIL® ENCRYPTION PROTOCOLS

- ChatMail's Advanced Messaging & Parsing Protocol (CAMP)
  - Encrypted email is displayed as chat message
  - Interface auto identifies users: internal (blue) & external (grey)
  - Data never stored in plain text
- Diffie-Hellman Key Exchange & Curve25519
  - Public cryptographic keys
- PGP Encryption
  - Ability to cross-communicate with other PGP platforms
  - Private PGP keys randomly generated on device storage
- Message authentication codes: HMAC based on SHA256
- Symmetric encryption: AES-256 in counter mode (CTR)
- Verification using public identity key
- Control over message delivery system: no roster, group, or message storage
- Encrypted calling
  - Zimmermann Real-Time Transport Protocol (ZRTP)
  - Transport layer security (TLS) ECDHE X25519

CHATMAIL FEATURES

- Encrypted group calling
- Anonymous group chat
- Encrypted notes & notebook lock
- Crisis controls: remote wipe, duress password, Destroy ChatMail
- Multiple languages
- Encrypted camera & photos
- Private key security
- Unified user interface

CURRENCY CONVERTER

- Supports major currencies & cryptocurrencies
- Search bar for your preferred currencies
- Compare currencies side-by-side
- Historical reference charts
- Only communicates with private data center

CALCULATOR

- No external connections
- Essential math calculations
- No history, storage, or recovery