# Bittium Secure Suite™
## Full set of services for secure communications


**Bittium Secure Suite** provides a full set of services for secure communication, data transfer, and device management when using ultra secure Bittium Tough Mobile 2 smartphones or other Android™ or Microsoft Windows devices. With Bittium Secure Suite, you do not need to rely on public Internet connectivity, third parties or cloud services.

Operate and control all the Secure Suite services on your secure premises, or use a trusted operator to host the services. The single step provisioning with QR codes enables seamless and easy deployment of the Secure Suite services for your device fleet.

Together with Tough Mobile 2 smartphones, Secure Suite forms the world's most secure mobile communication solution that has been approved up to CONFIDENTIAL (NCSA-FI, TL III) and NATO Restricted level communications.

FOR MORE INFORMATION, PLEASE CONTACT:
salesglobal1@bittium.com

## Benefits

**Secured Network Traffic**
With Bittium SafeMove® Mobile VPN

**Efficient Control Over Device fleet**
With Mobile Device Management feature

**Approved Applications Only**
Enterprise library and mobile application management

**No Data Leaks**
Access to services granted only for devices that have been remotely attested for integrity

**Always up-to-date**
Firmware and application updates delivered to Bittium Tough Mobile 2 over-the-air

**Undeniable Audit Trail from Devices**
Audit trail from devices and server components with Log Server

**Works in private and closed networks**
Secure push messaging to devices without the risks of public clouds

# Bittium Secure Suite™
# Technical specifications

## Mobile VPN Features

- IPsec, IKEv2 MOBIKE
- Integrated firewall and IPsec policy
- Always-on, cannot be bypassed by apps or user
- Require successful remote attestation for VPN access
- Per-app and per-container VPN
- Extensively tested and externally audited code base
- VPN tunnel for USB tethered traffic

## Mobile VPN Crypto

- CNSA/NSA suite B compatible
- SHA2-512
- AES-256, SERPENT
- Elliptic curve cryptography:
  - ECDH groups 19,20, 21 (NIST) and 27,28,29 and 30 for IKEv2 (Brainpool)
  - ECDSA certificates
- Hardware accelerated crypto

## Mobile Device Management

Centralized, remote management of the Tough Mobile 2 and Android security features from the server.

- Remote policy update (push)*
- Remote wipe, lock and password change*
- Manage trusted CA certificates*
- Factory reset protection*
- Android Enterprise support*
- SafeMove VPN policy management
- Device history and audit logs
- Wi-Fi management: SSID configuration, security policy and credentials
- Mass provisioning by operators, or self-provisioning by end users

*Only for Android devices

## Device Policy (Android)

- Device lock password policy:
  - Numerical, alphanumeric, complex
  - Password length
- Altogether, it is possible to control a total of 100+ parameters
- Device wipe after failed password entry
- Device lock timeout
- Password expiration time
- Wallpaper and owner info management
- Enable/disable:
  - Software from untrusted sources
  - Android Debugging Bridge (ADB)
  - Developer settings
  - Bluetooth
  - Camera
  - MMS send and receive
  - Location services
  - iZat (Qualcomm AGPS)
  - Android connectivity check
  - Volume adjustment
  - Application settings control
  - Cell broadcasts
  - Configuration of device credentials
  - Configuration of mobile networks
  - Tethering
  - Configuration of VPN
  - Configuration of WiFi
  - User-initiated factory reset
  - Apps installation and uninstallation
  - Modify accounts
  - Mount external physical media (USB, SD card)
  - User-initiated network settings reset
  - Outgoing NFC beam
  - Outgoing calls
  - SMS
  - Microphone volume adjustment
  - USB file transfer
  - USB whitelist

## Mobile Application Management (Android)

- Managed private application library from Bittium
- Managed public application library from Google Play
- Configuration of 3rd party apps (Android managed configurations)
- Application install base kept up-to-date with new versions and security fixes

## Bittium Secure Call™ (optional)

- End-to-end encrypted voice calls
- End-to-end encrypted video calls
- End-to-end encrypted messages
- Centralized Contact Directory

## Certificate Authority (CA)

- Includes production grade CA system
- EST and SCEP protocols for certificate enrollment to devices
- Automatic over-the-air renewal of certificates
- Integration with external CA systems

## Log Server and Visualization

- Visual log analytics for efficient incident response and even proactive incident avoidance
- Collecting and analyzing log data for keeping administrators up-to-date on what happens on device and infrastructure side
- Integrates with Bittium SafeMove® Analytics (optional)

## Secure Push Messaging

Secure and scalable push system that can be easily implemented in apps. Familiar API, similar to common cloud messaging systems.

- Low power requirements
- Low latency
- Low bandwidth
- Can be hosted on customer premises
- TLS security and optionally VPN

## Supported Server Platforms

- SafeMove Server Appliance
- VMware virtual appliance
- Common cloud and virtualization platforms

## Supported Client Platforms

- Android 9 onwards
- Microsoft Windows 10 onwards

**Bittium** • Ritaharjuntie 1, FI-90590 Oulu, Finland • Tel. +358 40 344 2000 • **www.bittium.com**