Bittium Secure Mobile Communication Solution

Bittium

The World's Most Secure Mobile Communication Solution

Bittium provides the world's most secure mobile communication solution for securing demanding governmental and enterprise communications. The solution is designed and built for combating the threat of unauthorized access to your organization's confidential data. The threats originate from different sources, such as malware, eaves-dropping, lost or stolen devices, device modification or cloning, user errors, and information collected by third party service providers.

Bittium's secure mobile communication solution includes Bittium Tough Mobile product family's Bittium Tough Mobile™ or Bittium Tough Mobile™ 2 smartphones and Bittium Secure Suite™ providing a full set of services for secure communications. Together the elements form the world's most secure mobile communication solution.

The best method to build the most secure mobile communication solution is to build it in layers. Bittium's solution is based on the combination of hardware and software, where each layer enhances the overall security. The security is further enhanced with trusted manufacturing located in Finland.

FOR MORE INFORMATION, PLEASE CONTACT:
sales1global@bittium.com
www.bittium.com

Bittium Secure Mobile Communication Solution

Benefits

Certified security
The solution with Bittium Tough Mobile is approved for storage, processing and transmission of data classified up to RESTRICTED and CONFIDENTIAL levels (NCSA-FI).

Data at rest secured
Critical data physically protected on the world's most secure mobile platforms. Security integrated deep within the hardware and source code to prevent extraction of data.

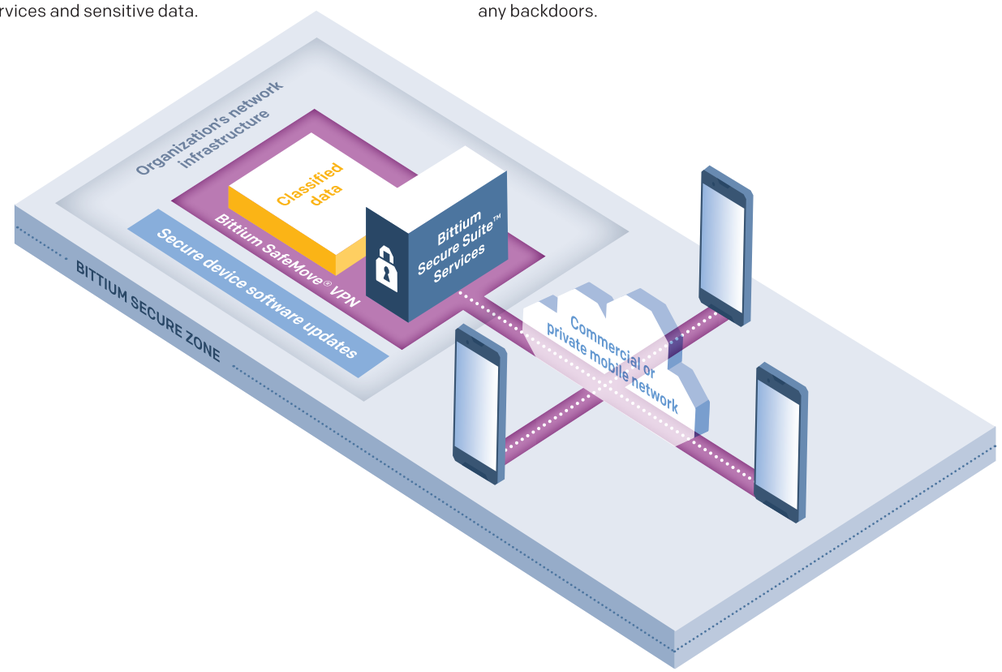
Data in transit secured
Encrypted network traffic, mobile device management and mobile application management from the Bittium Secure Suite management system.

Guaranteed device integrity
Bittium Tough Mobile product family's smartphones are manufactured in a controlled production line located in Finland and the integrity of the devices can be verified throughout their lifespan.

System Overview

Bittium Secure Mobile Communication Solution provides end-to-end encrypted access to organization's classified data and services. Your organization's network infrastructure can be seen as a network-wide secure zone utilizing Bittium's solutions to create a trusted access to your services and sensitive data.

The network-wide secure zone can be deployed either on commercial or private networks as the solution has no dependency on the public internet services. It can be hosted entirely by your organization, according to the security standards of your premises and without any backdoors.



Elements

Bittium Tough Mobile™ & Tough Mobile™ 2
Ultra secure smartphones

Security layers built on top of each other starting inside the device for keeping your confidential data safe.

- **HW secure element** – Ensures your critical data on the device cannot be accessed by securely storing confidential and cryptographic data on the tamper-resistant hardware platform.
- **Secure boot & HW integrity check** – Automatically ensures the integrity of the device hardware components and software at device start-up.
- **OS integrity** – Integrity of operating system is checked also during device operation.
- **Disk encryption** – Protects your critical data on the device using hardware rooted AES-256 algorithm.
- **Tamper detection** – The device alerts if there have been any attempts to break in, and when necessary, automatically deletes all data from the device.
- **Trusted manufacturing** – Manufacturing in Finland in a controlled production line.
- **Privacy Mode** – Hardware-based privacy mode for disabling microphones, cameras, Bluetooth, and reducing sensor accuracy (available with Tough Mobile 2)

Bittium Secure Suite™
Full set of services
for secure communications

Enabling high level of security for your communications, data transfer and device management.

- **Mobile VPN** – Securing your network traffic with the always-on Bittium SafeMove® Mobile VPN.
- **Mobile device management** – Efficient management and control of your device fleet.
- **Mobile application management** – Make available only the applications you approve for your users.
- **Remote attestation** – Prevent data leaks by granting access to critical information to only those devices whose integrity is remotely attested.
- **OTA firmware update** – Avoidance of data breaches with latest updates for Bittium Tough Mobile.

Solutions

For CONFIDENTIAL security level

- **Bittium Tough Mobile dual-boot** – Confidential use with Bittium Secure OS and personal use with hardened Android™. Full data separation between the two operating systems.
  - Two-factor user authentication with PIN/ password + NFC token*
  - Secure data containers for classified data
  - Improved cellular network security
- **Bittium Secure Suite** – Enhanced hardening to meet CONFIDENTIAL level requirements.
- **Encrypted calls & messaging** – Optionally available with an encrypted communication solution.

For RESTRICTED security level

- **Bittium Tough Mobile** – Without Google apps pre-installed
- **Bittium Secure Suite** – High level of security for data in transit and device management.
- **Encrypted calls & messaging** – Optionally available with an encrypted communication solution.

For high level of security

- **Bittium Tough Mobile or Bittium Tough Mobile 2** – With or without Google apps pre-installed
- **Bittium Secure Suite** – Optionally available for high level of security for data in transit and device management.
- **Encrypted calls & messaging** – Optionally available with an encrypted communication solution.

*YubiKey 5 by Yubico

Bittium

Connectivity
to be trusted.

Bittium / Ritaharjuntie 1, FI-90590 Oulu, Finland / t. +358 40 344 2000 / www.bittium.com