

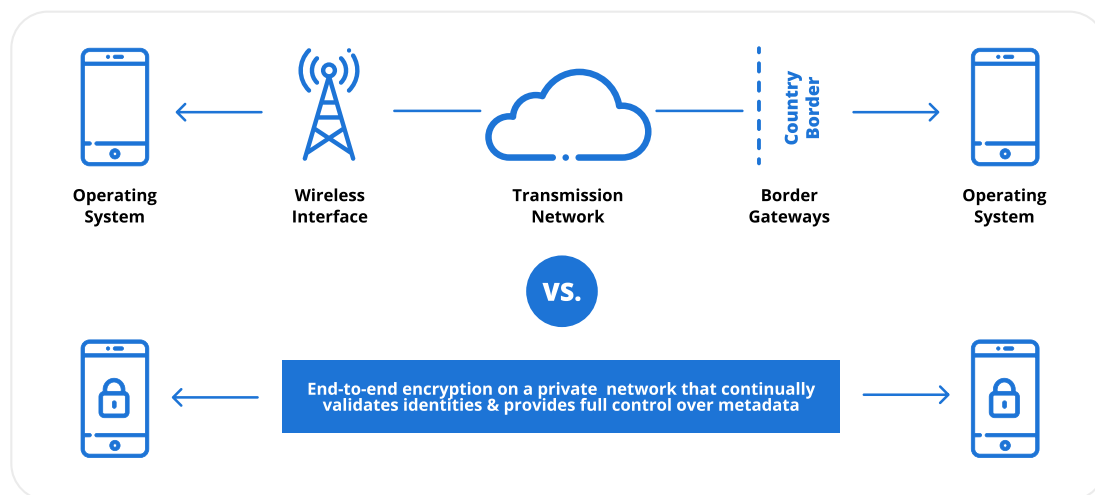
BlackBerry SecuSUITE

A multi-platform solution for end-to-end encryption of voice calls and messages.

SecuSUITE features a mobile application that allows users to conduct secure voice and data communications using off-the-shelf devices, including most commercially available phones running iOS and Android.

The solution takes the complexity of specialized hardware out of the picture, vastly improving ease of use and mission flexibility.

End-to-End Encryption



Solution Benefits

- **Continuous User Authentication** – solution cryptographically authenticates all users, so you can always rely on the in-built security to know who you're talking to, eliminating the risk of identity spoofing
- **Simple to Use** – it mimics a traditional phone client, complete with dial pad, call log, discernable secure call screen, and integrated text messaging
- **Native iOS CallKit** – it is integrated with the native iOS phone and contacts client, making it even more seamless for Apple users
- **Affordable** – saves money because calls can be made securely over readily available Wi-Fi connections without losing the integrity and security of the call
- **Eliminates Potential Threats from Malicious Adware, Robocalls, and Spam** — SecuSUITE is a closed network, so you'll always remain insulated and protected
- **Great Voice Quality** – audio quality that easily meets or exceeds what's available on commercial voice networks with minimal to indiscernible voice latency

Certifications

Common Criteria Certification. The SecuSUITE app for iOS, Android, and BlackBerry® devices has been certified according to the National Information Assurance Partnership (NIAP) Protection Profiles (PP) for SIP server and network devices.

NIAP Certification. SecuSUITE is an NIAP-certified voice solution that supports iOS and Android devices.

Approved by the CSfC Program under NSA specifications. SecuSUITE is designed to meet the requirements of the National Security Agency's (NSA) Commercial Solutions for Classified program.

Compliant with the Federal Information Processing Standard (FIPS). SecuSUITE meets the U.S. government's computer security standard for cryptographic modules.

Installation Options

The SecuSUITE solution can be installed on-premise, in a data center, or in-the cloud.

Deploy SecuSUITE in a Wide Range of Environments



Existing
datacenters



Government
clouds



Public
clouds



Local tactical systems,
like military vehicles or
police SWAT team vans

Intuitive Interface

The SecuSUITE mobile app interface is simple to navigate, just like commercially available Android or iOS apps. For highly sensitive communications, extra protections such as fingerprints or PIN numbers can be included and managed by the administrator.

Flexible Implementation and Management

- Download the mobile app from an iOS or Android app store, or through an MDM push.
- Complete activation by entering an activation code and a URL or by scanning a QR code.
- With SecuSUITE, you can do “out-of-band activation” to authenticate devices without having to send a text, avoiding the possibility of “man-in-the-middle” attacks.
- In most cases, organizations can use their existing mobile device management (MDM) system to deploy and activate SecuSUITE across their user base.

Ready for demo?

See BlackBerry's SecuSuite secure enterprise messenger in action.
Email blackberry@bakotech.com to arrange a demo.