BlackBerry's SecuSUITE

Solution Guide, January 2020

CONTENTS

THE RISK OF MOBILE COMMUNICATIONS

Today there are more mobile devices on the planet – some 7 billion – than there are people, spawning a trend that is challenging enterprises and governments worldwide: the rise of mobile cyberattacks. Increasingly, malicious hackers are tapping mobile networks to capture calls and messages, threatening the safety and security of business leaders, military personnel, and diplomats, and putting at risk the critical data they hold and share. In the current environment, organizations are struggling to keep control and ownership of metadata and to comply with tightening regulatory mandates.

Mobile Hacking is Easy and Common

Breaking into mobile networks is surprisingly easy and common. Hackers have become experts at identity spoofing and hijacking, while advanced snooping technologies are exposing sensitive communications to cybercriminals and foreign governments. The evidence is everywhere in the news:

- "Mass snooping fake mobile towers uncovered in UK" (BBC)
- "Washington, DC is littered with fake cell tower surveillance devices" (Wired)
- "17 fake cell towers discovered in one month" (Computerworld)
- "Fake mobile phone towers discovered in London" (Ars Technica)
- "Israel accused of planting mysterious spy devices near the White House" (Politico)

Encryption Can Help – Up to a Point

Traditional techniques for securing mobile communications – most notably encryption – have had some success in preventing interceptions, but serious vulnerabilities remain. Researchers at Black Hat USA's 2019 conference, for example, demonstrated how known vulnerabilities in WhatsApp could still be exploited by manipulating chats. And Wired Magazine showed how all it took was a phone call to hack WhatsApp.

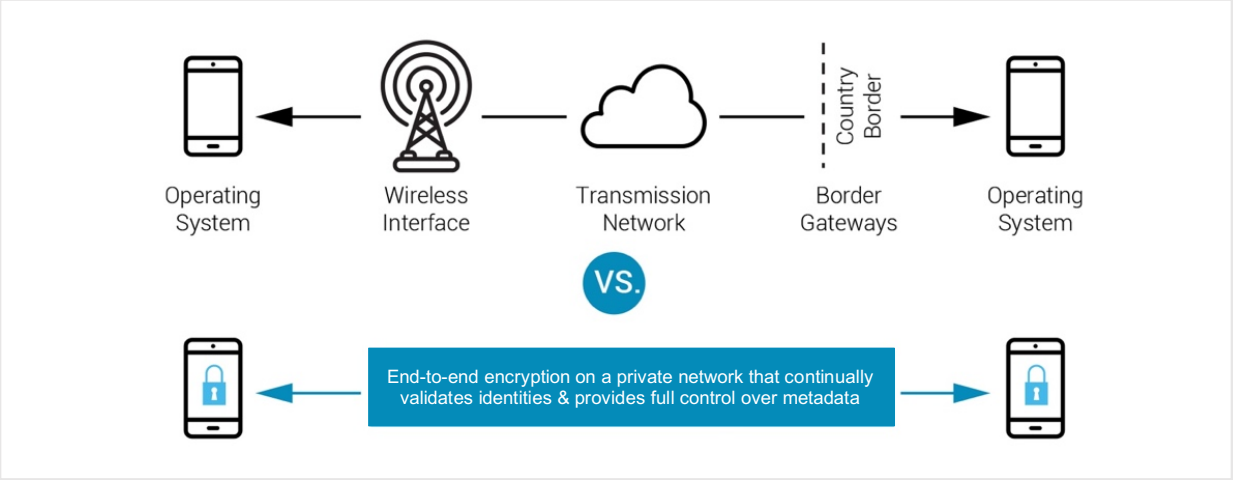
Bad actors have broken into the mobile communications of leaders worldwide. Brazilian President Bolsonaro's cellphone was hacked, and the FBI is investigating texts that impersonated U.S. Vice President Pence's press secretary sent to congressmen. Further, researchers have shown how easy it is to send fake presidential alerts to your phone.

THE SOLUTION: BLACKBERRY'S SECUSUITE

For governments and businesses worldwide, there is a better solution for ensuring security and protecting data across your mobile networks and devices. SecuSUITE® for Government is a multi-platform solution for end-to-end encryption of voice calls and messages. It is trusted by governments, world leaders, and business executives around the globe. Driving their trust is a wealth of certifications and independent approvals secured from multiple government agencies. No other voice communications solution has invested this much in meeting global security standards.

The SecuSUITE for Government solution keeps communications secure on Android™ and iOS® devices. Thanks to its ease of use, strong encryption, and easy installation and management, SecuSUITE for Government offers everything you need to keep your sensitive voice conversations secure.

End-to-End Encryption



Solution Benefits

- **High security voice and messaging for iOS and Android –** features a hardened mobile application that allows users to conduct secure voice and data communications using off-the-shelf devices
- **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

USE CASES: SECUSUITE IN ACTION

SecuSUITE transforms how people communicate anywhere in the world. It provides hyper-secure protections for government staff working in sensitive or dangerous locations — or any place where conversations can be intercepted by bad actors.

Real Life Examples

- **International –** The threat of cyberattacks and eavesdropping is extremely high when people are out of the country. In government circles, it is standard operating procedure to assume that all cross-border calls are being monitored or recorded. SecuSUITE provides an end-to-end secure system for communicating with co-workers in the home office and with others whose locations may not even be known.
- **Communicating with Out-of-Network Officials –** Government employees traveling or stationed overseas frequently need to communicate over a secure channel with officials and executives from other nations. SecuSUITE enables these employees to securely discuss sensitive topics with foreign officials.
- **Military Personnel Stationed Abroad –** SecuSUITE is an ideal system for enabling military staff posted in overseas locations to securely communicate from anywhere in the world using a regular mobile device.
- **Communicating with Contractors and Business Partners in Foreign Countries –** Government staff working in foreign countries frequently need to communicate with non-government contractors and other business partners. These partners can be issued temporary credentials to communicate with government employees without joining the government telephony network.
- **Corporate Executives on the Move –** High-level business executives can be exposed to hackers and cyberthieves when traveling out of country. With SecuSUITE, communications are always encrypted and secured back to their corporate home offices.

A Full Range of Communication Options

Mobile to Mobile

In this scenario, two people who are members of the same SecuSUITE secure private network communicate with each other from anywhere in the world over a secure network. Callers use SecuSUITE's end-to-end secure communication channel managed on premises or in the cloud.

From a SecuSUITE-enabled mobile device to SecuSUITE- enabled mobile device

- **Secure Landing**

  A person using the SecuSUITE mobile app can connect with a greater number of people by tying the call into a secure landline inside an agency or corporate network.

From a SecuSUITE-enabled mobile device to a landline within the agency network

- **Secure Conferencing**

  Mobile users of the SecuSUITE app can securely join a conference call over an agency or corporate PBX, allowing multiple individuals to share sensitive or secret information. SecuSUITE software provides encryption and security on both sides.

From a SecuSUITE-enabled mobile device to a secure conference bridge

- **Break-Out**

  In this scenario, a mobile user of the SecuSUITE app places a call into an office network, which is then routed via a public network (e.g., AT&T, Verizon) to a number outside the office. Security and encryption are assured from the mobile app to the home office — usually the most “exposed” part of the conversation when the caller is located outside the country.

From a SecuSUITE-enabled mobile device to the user’s home network and from there to external mobile or landlines via PSTN extension

- **Break-In**

  This is the opposite scenario from “break-out.” It’s when someone places a call from an unsecured public network into the user’s home government or corporate

office network. The call is then securely routed to a user of the SecuSUITE mobile app, regardless of where in the world the SecuSUITE user is located.

From any mobile or landline on the user's home network to a SecuSUITE-enabled mobile device

CERTIFICATIONS: MEETING THE STRICTEST GLOBAL STANDARDS

SecuSUITE helps organizations comply with a complete range of regulatory requirements around call and message metadata. Using the solution, customers can configure the collection and export of this data to automatically address specific government and industry regulations.

- **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.

CONFIGURATION AND SYSTEM OPTIONS: SECURITY MADE EASY

No matter how secure your communications system, it only works when people actually use it. And to ensure adoption, you need to deliver a compelling user experience. SecuSUITE is an easy-to-use, secure communications platform. Calling with the SecuSUITE app is like using your regular iOS or Android phone, but with added security.

When employees are on a sensitive mission anywhere in the world, they can leave behind those bulky specialized devices that stand out in a crowd. And there's no longer the need to go to a secure facility to make calls.

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.

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

Installation Options

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

- **On-premise** installations are typically done for customers wanting full control over their data and associated transmissions or for tactical installs in a standalone (closed) network environment.
- **Data center or hosted environments** would be used when a customer would like to have a vendor completely manage the SecuSUITE network at a vendor facility.
- **Cloud installations** such as AWS and Azure public and government clouds offer flexibility for expansion and customers can decide whether they need a self-managed hosted system or a vendor managed hosted system.

High Availability Configuration (Active-Passive)

The SecuSUITE system can operate in an active-passive configuration that ensures continuous service availability using RedHat High-Available Cluster. In this setup, a second (passive) SecuSUITE system instance runs in stand-by mode, which allows the passive machine to take over the service without loss of data if the active machine fails.

High-Level Features of the HA Configuration

- **Health Status Monitoring**: During operation of the active machine, several parameters such as disk space, CPU load, and memory usage are continuously monitored and can be reviewed by the system admin. When certain conditions are met, an automatic switch to the passive machine is triggered.
- **Database Sync**: The database of the active machine is synchronized to the passive machine at regular intervals to ensure that the passive machine can take over operations at any time.
- **Automatic and Manual Hand-Over**: The cluster service tool allows for automatic and manual hand over of the service to the passive machine. During the failure state, the admin can investigate and eliminate the root cause for the failure and afterwards switch back the operation to the initial state. The manual switch can also be used when maintenance/upgrade work is required.
- **Notification Alerts:** The SecuSUITE system can be configured to send email alerts to the system admin. The alerts are sent out when a failure is detected and after a successful switch.

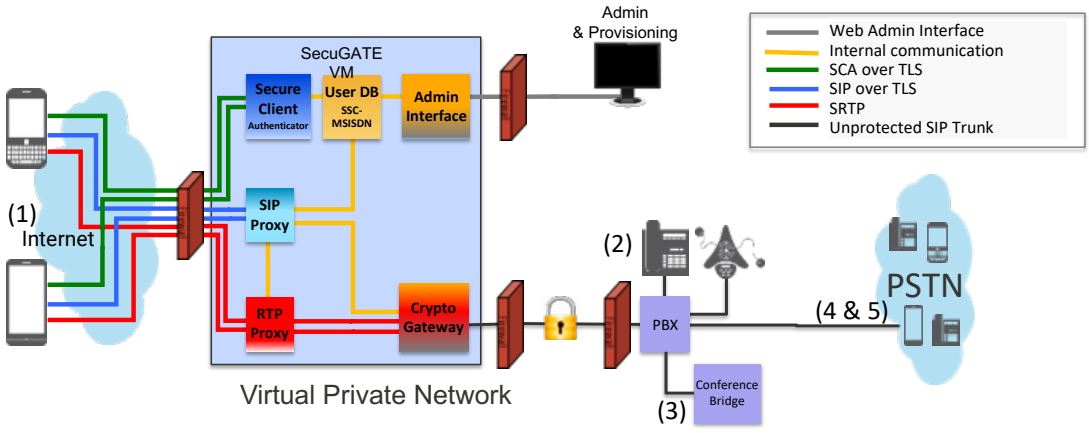
ARCHITECTURE & SECURITY LEVELS

SecuSUITE mobilizes secure voice and text communications to protect against threats to security at all communication levels from Sensitive But Unclassified (SBU) and Controlled Unclassified Information (CUI) to Top Secret.

SecuGATE Architecture

SecuSUITE creates a hyper-secure network connection between every user of the application. Underpinning the solution is BlackBerry's secure server, SecuGATE™, which authenticates users and creates a fresh pair of encryption keys before sending the voice and data through the SecuSUITE app. Both the SecuSUITE client and the SecuGATE server have been independently tested and approved for use on U.S. government devices.

Think of SecuSUITE as a private, highly secure, end-to-end communications network. Only authorized members of the network can use the SecuSUITE app to communicate with each other. Behind the scenes, an administrator controls membership in the network and determines who can access and use the application.



CUSTOMIZABLE TECHNICAL SUPPORT IN YOUR TIMEZONE

BlackBerry® Technical Support Services (BTSS) provides organizations with direct access to a team of technical experts at BlackBerry in order to help achieve maximum uptime and stability of BlackBerry enterprise software. With a flexible choice of program levels and optional services designed to meet the needs of organizations - regardless of the size and complexity of your BlackBerry enterprise software deployment - there are Support and Services options that will help provide your organization with increased productivity.

Support Levels

The BlackBerry Technical Support Services program is divided into two support levels – Advantage Support and Premium Support.

- **Advantage Support** provides Administrator access to technical support for customers who have a significant or growing number of managed mobile devices. Advantage Support is designed for small to medium sized organizations that require assistance with technical and/or configuration issues in a timely manner to help ensure their organization is not negatively impacted by downtime.
- **Premium Support** provides enterprise grade, relationship-based services, for customers running a mission critical BlackBerry deployment. Customers at this level of support typically rely extensively on the BlackBerry enterprise solution and desire improved call routing to more experienced technical resources and improved response time targets. Premium Support offers 24x7 telephone access to our Direct Advanced Response Team (DART), a group of tier 3 technical experts with a broad knowledge of BlackBerry enterprise solution, and access to specific details about the customer's deployment.

Preventative Services: Premium Service Manager (PSM)

The Premium Service Manager (PSM) is a designated resource, assigned by BlackBerry, to build an ongoing relationship with the customer's BlackBerry administration resources. The PSM will be the customer's internal advocate at BlackBerry, act as the first point-of-contact for escalations of support-related issues, and liaise with other BlackBerry teams on behalf of a customer where appropriate. The PSM will be available from 8am to 5pm, Monday to Friday in a single time zone (as designated by the customer).

Common PSM Tasks

- **Annual onsite visit.** The PSM will visit the customer's primary location annually.
- **Weekly customized reporting.** The PSM will provide customized reports on a regular basis that may include: open issues and status, closed cases, pending software updates, top server issues.
- **Weekly communications.** The PSM will arrange regular conference calls to review reports and provide proactive technical notifications as they become available.
- **Ongoing customer advocacy.** The PSM will act as a point of contact to help connect the customer with other internal BlackBerry resources as needed.