Truly Secure Voice, Text, and Data Communication

Organizations depend on their ability to communicate from anywhere at any time. They often do so, however, with a false sense of security, trusting the safety of calls and text messages sent from their mobile devices. In fact, mobile devices and networks are highly vulnerable and easily compromised, putting personal safety and the confidentiality of business information at risk. Isolating mobile devices from these risks is essential to safeguarding your people, your clients, and your information.

SAIFE® Mobile solutions provide secure, encrypted voice, text, multimedia messaging, and data sharing over commercial and private cellular networks, public and private Wi-Fi, and satellite. SAIFE Mobile solutions are easy to install, easy to manage, and seamlessly operate across Android™ and iOS® devices.

SAIFE's complete mobile communications solutions transform commercially available, off-the-shelf (COTS) Android and iOS devices into highly secure devices that protects an organization's sensitive communications and information.

SAIFE Mobile: Secure Voice, Text, Multimedia Messaging

SAIFE Mobile enables secure voice and SMS/MMS messaging among pre-authorized, pre-authenticated COTS Android and iOS devices. SAIFE Mobile apps are easily downloaded and activated, and require no additional hardware. Secure voice calls are placed and secure text messages sent in a similar manner as conventional calls and messages – no special training is required. Whether securing communication among executives or groups within an organization, or creating an impermanent cross-organizational working group, SAIFE Mobile is a cost-effective, proven solution.

Communication Groups. SAIFE Mobile employs the concept of Groups to allow secure communications exclusively among members of a group. An organization can easily create groups and add and delete members from a group. Individuals can reside in more than one group, and groups may include individuals from other organizations enabling secure communities of interest that can be quickly and easily stood up or disbanded.

Zero Internet Visibility. SAIFE Continuum routes VOIP, SMS, MMS, and data packets over the network cryptographically without exposing IP addresses. Traffic analysis is defeated. Encrypted traffic cannot be analyzed to decipher communication patterns, pairing, profiles, or other intelligence.

Ease of Use & Management. SAIFE Mobile is easy to deploy and easy to install. Devices can be rapidly provisioned along with designated contacts that are automatically loaded. Provisioned devices can be easily managed using the SAIFE Deployment Manager, and lost or stolen devices can be instantly revoked.

End-to-End Security. SAIFE Mobile dynamically establishes secure tunnels through the network via SAIFE Continuum in which the privacy and integrity of traffic for every session is assured inside a micro-perimeter. SAIFE Continuum allows only pre-authorized, pre-authenticated connections and employs FIPS 140-2 compliant, end-to-end 256-bit AES encryption. Key management is fully automated. Private keys are generated on and never leave the device. Meaningful communication can only occur between initiator and intended recipient. Untrusted devices cannot establish a trusted connection – no eaves dropping, no call interception.

Cross Platform Compatibility. SAIFE Mobile is available for both Android and iOS, as well as Windows® PCs and macOS® devices with full-cross platform interoperability. Encrypted calls and messages can be exchanged regardless of device type.

Network Flexibility. SAIFE Mobile was designed for high performance over low quality networks and works over public and private Wi-Fi, satellite, and commercial and private cellular networks.

SAIFE Command: Secure Mobile to Desktop Communications and Device Management

SAIFE Command is a powerful visualization, management, and communication desktop application. SAIFE Command's integrated VoIP client enables secure voice and text communications and image sharing among desktop and mobile devices. Its device management features include the ability to create and manage groups, provision and manage endpoints (smartphones, tablets, laptops), and view their precise locations in real-time. SAIFE Command operates on both macOS and Windows 10 devices.

SAIFE Command provides:

Secure Cross-Platform Communications. SAIFE Command enables secure, real-time voice, SMS, group messaging, and file transfer between administrators and end users with SAIFE Mobile equipped Android and iOS devices.

Location Tracking. SAIFE Command provides real-time location monitoring of end-users in the field, displaying device location on a map.

Device Management. From mobile device provisioning, configuration, and revocation to creating and managing communication groups, administrators can easily view and manage their organization's SAIFE Mobile enabled devices through SAIFE Command's intuitive interface.

SAIFE Connect: Secure Data Communication

The SAIFE Connect client application enables secure data communications and file transfer between mobile devices and network services over untrusted networks. SAIFE Connect is easy to install on Android and iOS devices, and works seamlessly, protecting valuable data in transit by making it invisible to potential attackers.

SAIFE Mobile Specifications

AVAILABLE PLATFORMS
Android™ 5.0+, iOS®

SUPPORTED NETWORK TYPES
Wi-Fi (public and private), cellular 3G/4G (commercial and private), satellite

SERVICES
VoIP, SMS, MMS

ABOUT SAIFE

SAIFE eliminates the inherent vulnerabilities of traditional perimeter defenses that cost organizations hundreds of millions of dollars in breach-related losses every year. We are redefining perimeter security, enabling secure, trusted access to services and data sets over untrusted networks, while making those same services and data sets invisible to unauthorized users and would-be attackers. We've extended the concept of a Software Defined Perimeter to create the first solution that enables dynamic, agile, network overlay perimeters that are device, user, and application-centric, and which can span on premise, cloud, mobile devices, and applications. SAIFE protects customers by substantially lowering their attack surface and enables information sharing across untrusted networks to reduce third-party risk.

As the world gets more interconnected, it becomes smarter, more aware, more productive — and more vulnerable, our job is keeping it **SAIFE**.

SAIFE