GO-TRUST ANDROID ENCRYPTION SUITE

Everything you need to keep all your Android Smart Phone business and personal communication and information totally secure.

The one and only military strength hardware encryption solution for Android phones and pc tablets

The GO-Trust Android Encryption Suite encrypts your Voice, your SMS and Instant Text communication. Your Pictures and other Confidential Files are also encrypted and safely stored on your phone, your microSD card or using cloud storage. Only you can retrieve them.

The Android Encryption Suite uses a powerful 32-bit Hardware Security Module (HSM) built into a microSD form factor. This design means you can use your existing Android Smart Phone (Release 2.1 or later) for military strength communications. No modification is required to your phone or the Android operating system.

Just insert the GO-Trust microSD (SDencrypter) in your phone, install the GO-Trust application stored on the flash memory on the microSD and you are ready to use Military Strength Encryption.

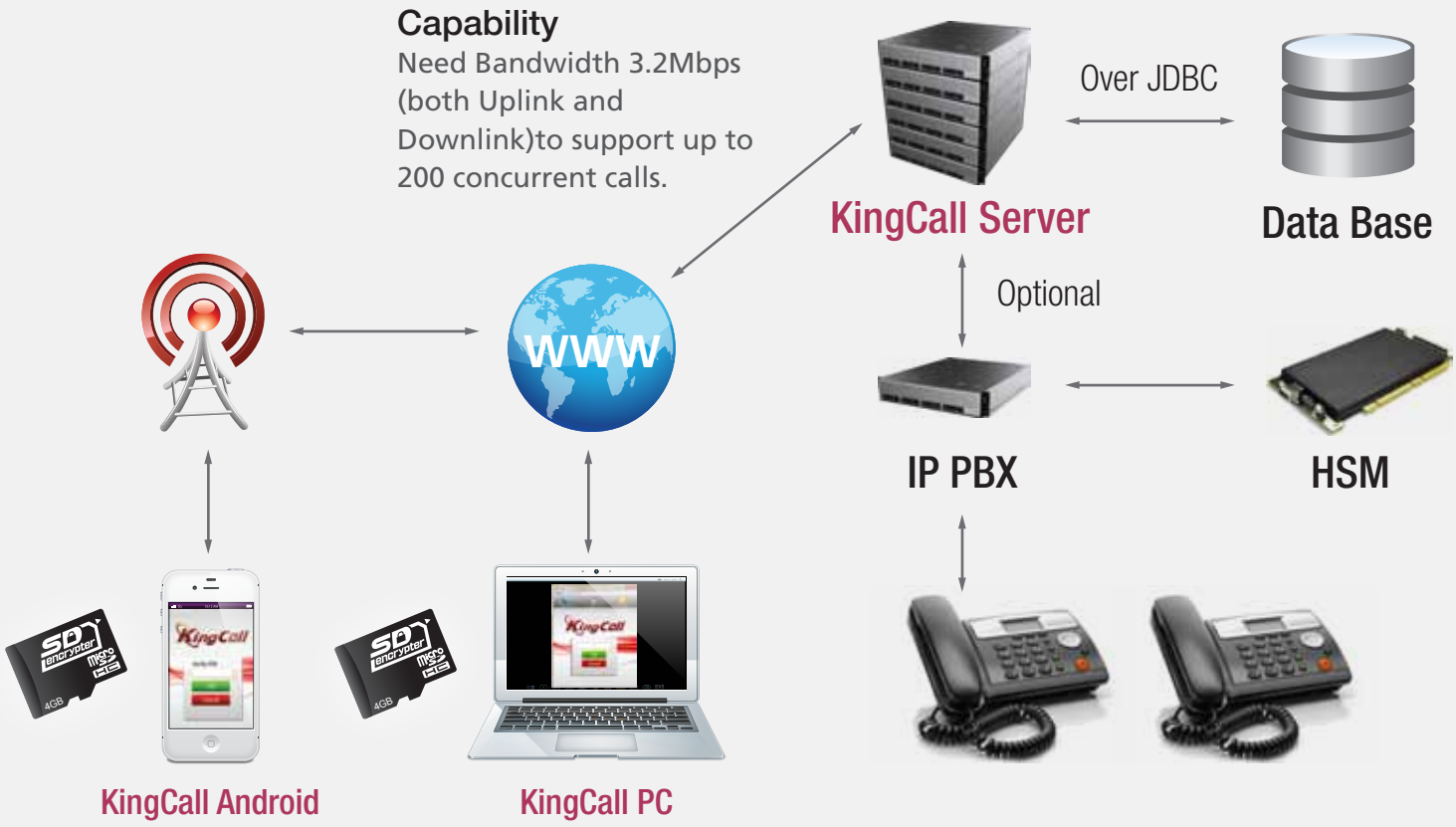
Two products make up the Android Encryption Suite, they can be purchased separately or as a complete suite (KingSuite).

SMS text scrambling between private groups of Android Smart phone and Tablet PC Users for a low onetime charge. The SMS address book, stored messages (sent and received) and all history is encrypted and stored inside the microSD flash memory; and like KingCall they cannot be reviewed without your PIN even if the phone or microSD scrambler is stolen or confiscated. KingText also encrypts any data files or photographs you select and allows you to store them securely in the phone, on the microSD flash memory or using cloud storage.

Voice scrambling & instant messaging between private groups of Android Smart phone and Tablet PC Users. Groups can be as small as two people or communities of many thousands. Ideal for high profile personalities, boards of directors, road warriors or everybody in a company or organization. The address book and call history are encrypted and stored inside the microSD flash memory, they cannot be reviewed without your PIN even if the phone or the KingCall microSD is stolen or confiscated. (Five invalid PIN attempts and all your information is locked forever). KingCall – Android can also be installed on Windows Notebooks and PCs.

KingCall ENTERPRISE

Enterprise configurations are available with complete SIP server and RTP relay ownership. Bridging (gateway) options allow interfacing with existing office wire phones. Everything is100% under the corporate control.



KingCall Server Features

- SIP
- RTP Relay
- Registrar Service
- Call Routing
- NAT Traversal
- Dial Plan
- Authentication
- Session Management
- TCP Transport Support
- UPnP
- Presence Agent support - RFC 3856
- XCAP support for Presence Agent - RFC 4825
- Logging capabilities
- Support Radius Billing system

Security Features

protects against the exploitation of SIP protocol vulnerabilities, as well as SIP server non-vulnerability-based threats including:

- SIP server resource misuse
- SIP application brute forcing
- SIP Application scanning
- SIP application flooding

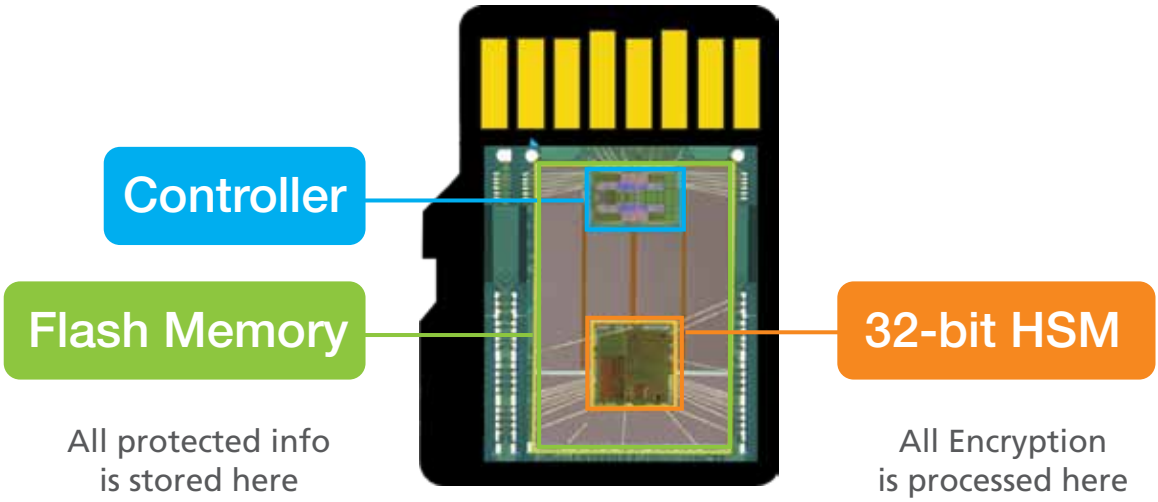
Requirement of DataBase

- MySQL recommended. Any other relationalData-Base will also work.

Hardware Security is inside a microSD

All your communications and files are protected by a military strength hardware security module embedded inside the microSD. No secure operations take place in the open in your smart phone's operating system, they all take place hidden deep inside the microSD.

Actual Size

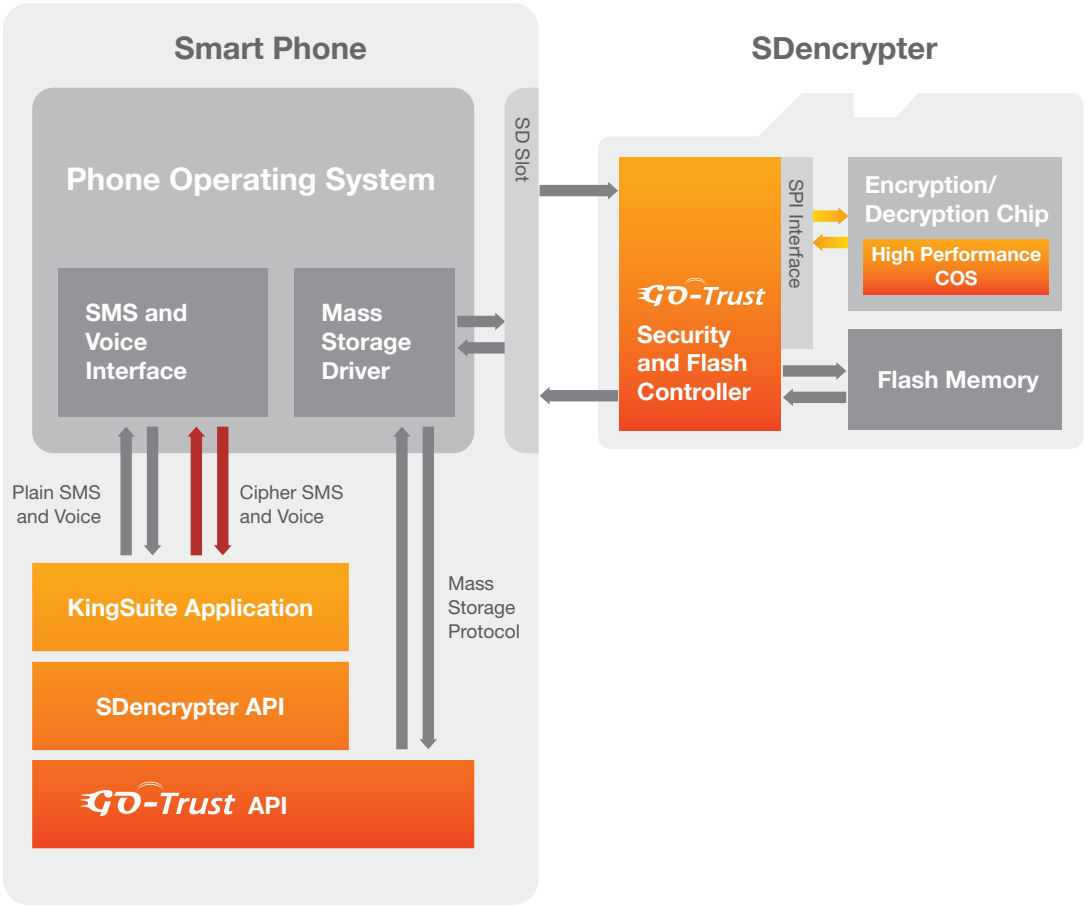


Technical Specification

- 32-bit Security chip inside the secure microSD is certified by Common Criteria EAL 5+
- In –Chip Crypto Operations: RSA 2048, SHA-256, AES-256, Key Exchange.
- AES encryption module is certified by NIST in the USA
- Secure microSD (SDencrypter) is under process of security certification of FIPS 140-2 Level 3 (military grade in the USA).
- RSA Key pair is generated by secure microSD and the private key is never exposed.
- No confidential keys are stored or computed in the device
- Voice encryption key (session key) is generated by a True Random Number Generator and exchanged by RSA and Diffie-Hellman.
- Voice encryption key is completely random and different for each phone call and instant messaging.
- Voice is encrypted by the AES-256 session key and the operation is done inside secure microSD.
- Security chip is able to withstand physical attacks.
- VoIP is based on standard SIP Technology. PC version works with Windows XP, Vista and 7.

KingCall Security

- A unique RSA key pair is generated when you first install the application. Your private key is securely hidden inside the Hardware Security Module (HSM) and nobody can see it, not even you.
- Each phone call session key is randomly generated just before the call starts.
- All session keys are encrypted and exchanged peer to peer; the SIP server never sees them.
- All encryption and decryption takes place in the microSD HSM, nothing is ever in the open inside the Android phone operating system. Even a Trojan would find nothing.
- The AES Encryption Module is NIST (National Institute of Standards and Technology) certified.
- The KingCall microSD is being validated for FIPS 140-2 Level 3 – Military grade security.



Against Trojan attack

Against man-in-the-middle attack

Against eavesdropping

Against physical attack

Product Features

Feature	KingSuite	KingCall	KingText
Voice Encryption	●	●	—
Instant message Encryption	●	●	—
Voice Address Book Encryption	●	●	—
SMS Encryption	●	—	●
SMS History Encryption	●	—	●
SMS Address Book Encryption	●	—	●
File and Photo Encryption	●	—	●
Secure Cloud Storage options	●	—	●
Military Strength Encryption	●	●	●
Also runs on Windows PC's	●	●	—
AES Encryption key length	256/128	256	128
New random key per session	● (KingCall)	●	—

KingCall PC

We have not forgotten PC Windows Users!

Voice scrambling between private groups of Windows Notebook or Desktop Users is also available without the Android Smart Phone installation option. Users can still communicate with Android Smart phone and Tablet PC Users so KingCall-Android and KingCall-PC users can be in the same private group. Security levels and information protection features are the same as for KingCall-Android.

SESAMES 2008 Sesames IT Security Winner

SESAMES 2011 Sesames Mobility Finalist

GO-Trust Trust in a Mobile World

GOTrust Technology Inc.

Taiwan

10F-1, NO. 306, Sec. 1, Wenxin Rd.
Nantun Dist. Taichung City 408, Taiwan

+886.4.2320.2525

USA

2522 Chambers Road, Suite 100
Tustin, CA 92780

+1.714.573.4051

For more information, please visit www.go-trust.com or email info@go-trust.com