seecrypt
COMMUNICATE IN CONFIDENCE

ENCRYPTION

Military-Grade Encryption for Secure Communication

Seecrypt provides secure voice calls, instant messages and file transfers between trusted mobile devices via high-grade, multi-layered encryption.

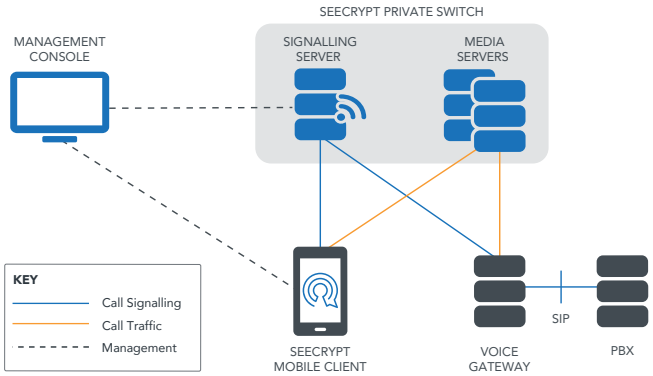
Protection of all communication and content is guaranteed by the Encrypted Mobile Content Protocol™ (EMCP), with real-time optimized delivery of encrypted content, even across low-bandwidth wireless networks.

Seecrypt uses standard encryption technologies including:

- Advanced Encryption Standard (AES) for symmetric encryption
- 384/256-bit Elliptic Curve Cryptographic Authentication
- Elliptic Curve Diffie-Hellman (ECDH) for key agreement
- Secure Hash Algorithm (SHA-2) for message digest

Seecrypt's Dual Cipher system uses double-wrapping for added security. Voice calls, for example, are first encrypted using ChaCha20 with a 512-bit key, followed by a second encryption again using AES with a 256-bit key.

SEECRYPT® ENCRYPTED CONTENT DELIVERY NETWORK



CRYPTOGRAPHY

Key Generation

- Entropy collected continuously from hardware sources -motion sensor, mic and OS sources e.g. /dev/urandom
- Long term ECC keys generated & stored in application's secure database
- No manufactured/generated key material is needed prior to use of the system

Voice Call Authentication

- Secure data exchange in two stages
- End-to-end standards-based key establishment providing mutual authentication, Perfect Forward Secrecy (PFS) and unique keys per-session
  - NIST SP800-56A C(2,2) Full Unified Model with Bi-lateral Key Confirmation
  - Authentication using NIST approved ECC curve P-384/512

Message Authentication

- End-to-end standards-based key establishment with mutual authentication
  - NIST SP800-56A C(1,2) One-Pass Unified Model
  - Public key fingerprint displayed in message dialog and contact details for vocal confirmation

Symmetric Cryptography

- Dual ciphers - ChaCha20 with 256-bit key and AES with a 256 bit key (FIPS SP 800-38)

Seecrypt is the global solution for trusted mobile communications, providing private, real-time messaging, voice/conference calling along with file sharing and transfer. Protected by leading-edge, authenticated, end-to-end encryption.

Combining military-grade security with the ease of use of a consumer app, Seecrypt requires no user training or configuration, ensuring fast and easy deployment, user acceptance and adoption across the enterprise.

With Seecrypt you can trust that your confidential mobile communications remain confidential.

CSG
COMMUNICATION SECURITY GROUP

www.seecrypt.com

email: info@seecrypt.com