Cellcrypt®
TRUSTED COMMUNICATIONS

Military-Grade Encryption for Secure Communication

Cellcrypt provides high grade, end-to-end encryption for secure voice calls messages and file transfers between trusted mobile devices.

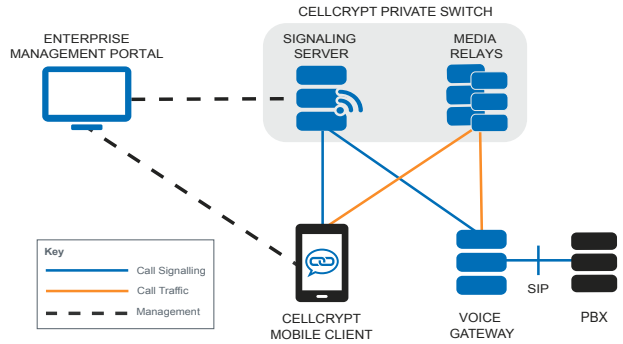
For protection of voice calls, instant messages and content, the Encrypted Mobile Content Protocol™ (EMCP) optimizes delivery of encrypted content in real-time, even across low-bandwidth wireless networks.

Cellcrypt uses standard encryption technologies including:

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

Cellcrypt's Dual Cipher system uses double-wrapping for added security. For example, voice calls are first encrypted using RC4 with a 384-bit key and then encrypted again using AES with a 256-bit key.

CELLCRYPT® ENCRYPTED CONTENT DELIVERY NETWORK



Cryptography

Key Generation

- Entropy collected continuously from hardware sources e.g. 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

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 - RC4 with 384-bit key and AES-CTR with 256-bit key
  - FIPS SP 800-38 – AES in CTR mode and AES in GCM mode (rev D)

NIST FIPS 140-2 Level 1 Certified

- Cellcrypt is certified to the FIPS 140-2 standard, approved by the US National Institute of Standards & Technology (NIST) (CERTIFICATE # 2575)

Cellcrypt is the complete solution for trusted mobile communications, providing secure, real-time messaging, voice/conference calling and secure file transfer, all protected by strong, authenticated, end-to-end encryption.

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

With Cellcrypt you can trust that your confidential communications remain that way.

DANMIK AGENCIES
email: info@danmik.com
www.cellcrypt.com.au