Cellcrypt®
PRIVATE SWITCH

Create your own, private, voice and messaging service

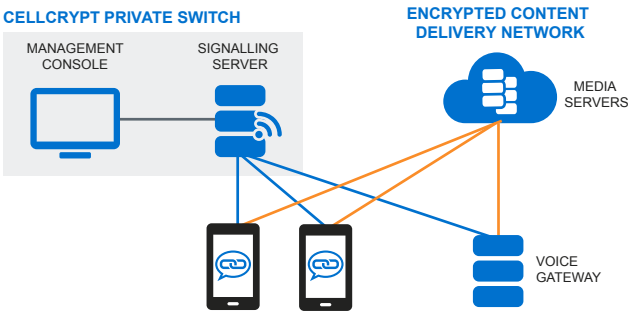
For complete security and control of your mobile communications

Cellcrypt's Private Switch is the core of control for Cellcrypt and is administered via a web-based management console with access restricted to authorized users.

It manages users; call signalling; call control and media communications and authenticates/authorizes every interaction within the network.

Cellcrypt Private Switch is designed to be used with the Encrypted Content Delivery Network – a global network of resilient and secure media servers for carrying call and message traffic.

ENCRYPTED CONTENT DELIVERY NETWORK™ (ECDN)



Private Switch Infrastructure

Signaling Server

- Handles authentication and call set-up for each client
- Includes Enterprise Management Portal to manage and control all devices and users on the Cellcrypt network

Media Server

- Routes encrypted packets between two devices involved in media session
- Media Relays operate outside the Cellcrypt Network and are deployed in multiple locations around the world in order to reduce latency in media sessions
- No user identifiable information or metadata regarding any media session is recorded by the media relays
- Ensures packets are correctly delivered on networks with poor performance

Management Console

- A web-based account management system for Cellcrypt
- Manage profiles, accounts, devices, subscriptions, and aliases
- At a glance dashboards and detailed reporting

On Premise or in the Cloud

The Cellcrypt Secure Switch infrastructure can be installed and operated fully on-premise within your data center or can be hosted as a cloud-based solution for reduced infrastructure and running costs.

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

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.

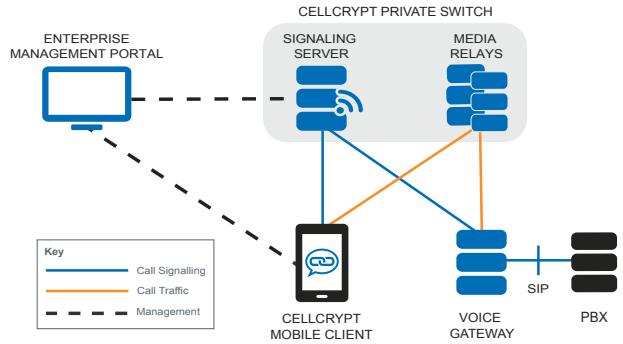
For protection of voice calls, instant messages and content, the Encrypted Mobile Content Protocol™ (EMCP) optimizes delivery of encrypted content in real-time, even across low-bandwidth wireless networks.

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