Cellcrypt®
TRUSTED COMMUNICATIONS

Secure Communications for Banking and Finance

Banks and financial organizations place great importance on winning, serving and retaining customers and are often early and rapid adopters of technology. Digital and online services, online banking, mobile check deposits, and account transfers have been around since the late 1990s.

While companies in other industries are exploring innovative new ways to connect with their customers, many banks are falling behind, as they are rightly cautious about how they communicate with their clients, especially high-networth individuals.

Most banks and financial institutions want the same things:

- Use secure instant messaging as means of communicating with their customers, including high-net worth, private banking clients
- Make encrypted calls directly with customers on their mobile phone, wheverever they are, without incurring costly mobile charges for the bank or the customer even when the client is travelling or is resident in another country
- Securely send and receive account related correspondence directly to the user's mobile device or PC/Mac
- Avoid, lengthy security question and answer sessions at the start of the call to identify and authenticate the client
- A secure mechanism for the client to authorize a financial transaction on their mobile device, anytime, anywhere
- For all communications, voice and data, with the customer to be fully protected against eavesdropping or interception

Cellcrypt's full range of services can be enabled within the existing IT and telecoms infrastructure, avoiding the need for an expensive rip-and-replace strategy.

Complete Privacy and Trust for Bank/Client Communications

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

Combining high-grade security with the ease of use of a consumer app, with Cellcrypt you can talk to your most sensitive and valuable clients with the knowledge and peace of mind that your messages and voice calls are completely private.

Cellcrypt requires no customer training or configuration, ensuring fast and easy acceptance, and the product can be white-labelled in your banks's brand idenity to ensure customer confidence.

Eliminating the need for lengthy challenge/ response identification substantially improves the customer experience the customer experience, while call times are reduced, resulting in significant costs savings for the bank.

Cellcrypt also provides a cryptographically secure one-time-PIN (OTP) functionality that enables a customer to authorise a financial or other account transaction directly from their mobile device.

Strong Encryption for Voice, Messaging and File Sharing

Cellcrypt leads the industry in delivering multi-layered, high-grade encryption for voice/ conference calls, instant messaging and file sharing. The platform utilizes standards-based protocols for optimized delivery of encrypted real-time content between mobile devices even across low-bandwidth wireless networks.

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.

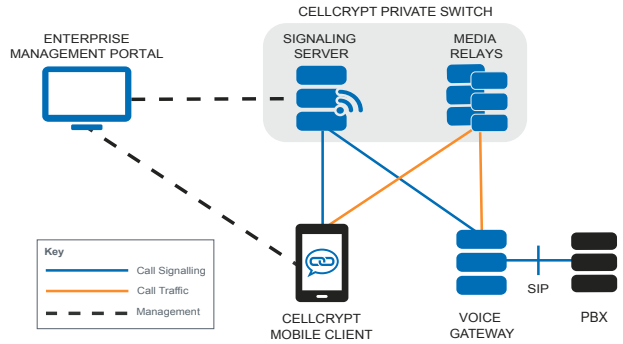
For protection of voice calls, instant messages and content, the Encrypted Mobile Content Protocol™ (EMCP) optimizes delivery of encrypted content in real-time, even across low-bandwidth wireless networks.

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