Cellcrypt

Cellcrypt Mobile for iPhone

Speak with confidence on your mobile phone

Cellcrypt Mobile™ for iPhone® makes your voice calls private and secure, so you can speak with confidence, wherever you are.

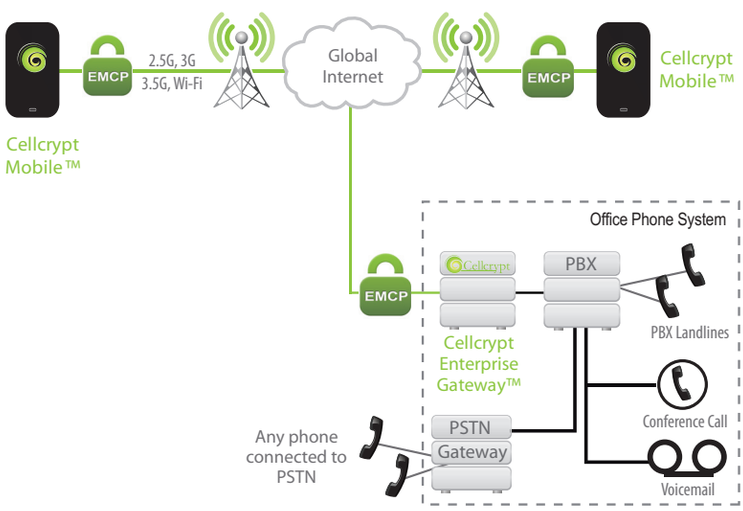
Protecting Valuable Information

Organisations make significant efforts to protect their valuable data from loss or interception – particularly when accessed outside the office and travelling abroad.

In 2010 the cost of mobile phone interception is significantly reduced since hackers computed and published free on the internet a codebook to decrypt GSM calls[1] – used in 80% of mobile phones worldwide – as well as demonstrating interception equipment that is readily available for under $2,000[2].

With Cellcrypt, calls can easily be protected on popular cell phones – and securely connected to office phone systems – so that you can be assured conversations remain confidential wherever they are.

End-to-end security on everyday mobile phones



Speak With Confidence

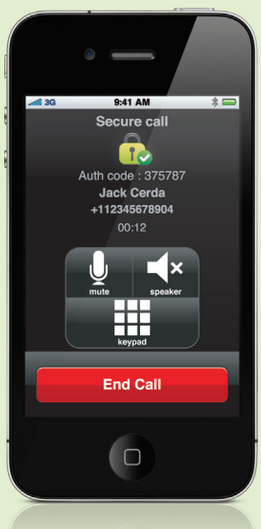
Cellcrypt Mobile for iPhone is an easy-to-use, next generation software solution that uses the data network to serve up unparalleled voice quality, low voice delays (latency), global coverage and intercontinental call capability - all delivered securely.

Using Cellcrypt Mobile is as easy as making a normal call, yet provides the confidence that phone calls, whether in the mobile or office environment, at home or overseas, within or between departments, suppliers and business partners, are protected end-to-end.

Security is assured; Cellcrypt uses the same well-established and trusted encryption technologies to protect voice communications that are used to protect laptops, corporate data and financial services transactions.

Key Features

- **Security**
  - Strong end-to-end encryption
  - US Government FIPS 140-2 validated (cert number 1310)
- **Simplicity**
  - User-installable application that runs on iPhone
  - No specialist equipment required
  - Intuitive user experience, runs in background & integrates with device phonebook
- **Performance**
  - Interoperates across and between leading smartphones and cellular networks
  - High call quality with low latency
  - International calling in over 200 countries
  - Secure calling to landlines with Cellcrypt Enterprise Gateway™
- **Network Support**
  - Any IP-enabled network, e.g.
    - GSM/CDMA
    - 2G
    - 3G
    - 4G
    - Satellite
    - Wi-Fi™



Cellcrypt Mobile for iPhone

Speak with confidence on your mobile phone

Cellcrypt's Technology

Cellcrypt's advanced solution leads the industry in delivering multi-layered security to establish a high-performance encrypted voice call between trusted wireless devices. It utilises Encrypted Mobile Content Protocol (EMCP), a set of standards-based protocols for optimising delivery of encrypted real-time content between mobile phones over low-bandwidth wireless networks. Cellcrypt's products are certified to the FIPS 140-2 standard, approved by the US National Institute of Standards & Technology (NIST).

Cryptography & Random Number Generation

Cellcrypt uses standard encryption technologies including:

- Advanced Encryption Standard (AES) for symmetric encryption
- Elliptic-Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for key agreement
- Secure Hash Algorithm (SHA) for message digest

In addition, before these algorithms are processed, Cellcrypt uses additional algorithms for added security (double-wrapping). For example, the voice call is first encrypted using RC4-256 bit and then encrypted again using AES-256 bit.

Public Cryptography
(2048-bit RSA & ECDSA using curves with 384-bit prime moduli)
RSA and ECDSA are used for authentication. The key pairs are generated on the phone during the installation and are unique to each phone. A private key is never shared. The Elliptic Curve Diffie-Hellman (ECDH) and RSA algorithms are used for key exchange. The session key is only valid for one phone call and securely destroyed after use.

Symmetric Cryptography
(AES & RC4, both 256 bits)
Both encryption algorithms are used at the same time. The data packet is first encrypted with RC4 and the cipher text is then encrypted again with AES in Counter Mode (CTR). Both algorithms are initialised with the exchanged session key.

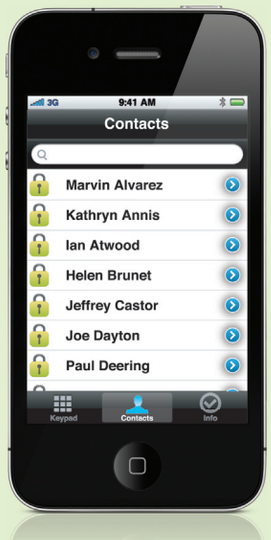
Hashing Algorithms
(SHA512)
Industry standard hashing algorithms are used for increased integrity assurance.

Random Number Generation
A 2048 bit seed pool is generated during the installation and is periodically updated. The initial seed is derived from the microphone input.

About Cellcrypt

Cellcrypt is the leading provider of encrypted voice calling on mobile phones. Founded in 2005 to develop high security encryption solutions for mobile devices, it developed Encrypted Mobile Content Protocol (EMCP) to solve performance challenges in the industry. EMCP is a standards-based technology that uses IP (internet protocol) to provide optimised delivery of encrypted data.

Today, Cellcrypt solutions are used routinely by governments, enterprises and senior-level executives worldwide. Cellcrypt is a privately-held, venture-backed company with headquarters in London, UK and offices in USA and Middle East.



Contact Cellcrypt:

Europe
13-15 Carteret Street
London, SW1H 9DJ, United Kingdom
Tel: +44 (0) 2070 995 999

North America
8300 Boone Blvd., Suite 500
Vienna, VA 22182-2681, United States
Tel: +1 (703) 879-3328

530 Lytton Avenue, 2nd Floor
Palo Alto, CA 94301, United States
Tel: +1 (650) 617-3219

Latin America
Latitude One,
175 SW 7th Street, Suite 1411
Miami, FL 33130, United States
Tel: +1 (786) 999-8425

Middle East & Africa
Bayswater Building, 20th Floor
Office 2002, PO Box 38255
Business Bay, Dubai, UAE
Tel: +971 (0)4454 1271

Asia Pacific
1 Fullerton Road #/02-01 One Fullerton
Singapore 049213, Singapore
Tel: +65 6832 5582

email: info@cellcrypt.com
web: www.cellcrypt.com

[1] "Mobile Encryption Code Is Divulged", New York Times, 29 December 2009 - [2] "Mobile Phone Hacking for £1000", computerweekly.com, 19 April 2010