Cellcrypt Enterprise Gateway

Connect securely to your office phone system

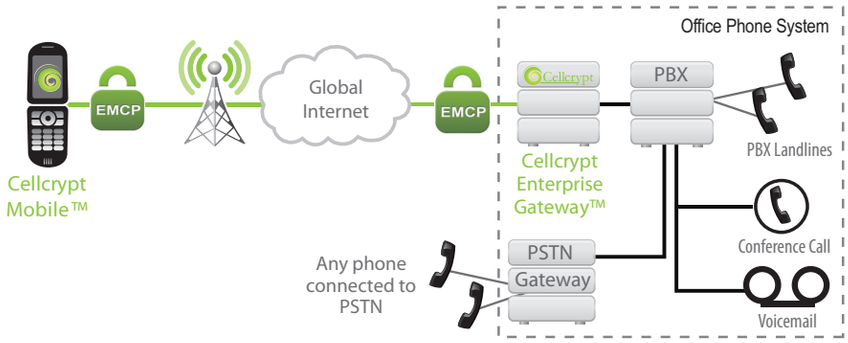
Cellcrypt Enterprise Gateway™ ensures you can connect with confidence from your mobile phone to your office phone system to call landlines as well as access PBX features such as voicemail, conference calling and calling out to the public phone network.

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.



Speak with confidence

Cellcrypt Enterprise Gateway is an enterprise software application that interfaces to office phone systems and encrypts calls to and from Cellcrypt-enabled mobile phones.

It provides a secure voice channel between Cellcrypt Mobile™ and existing office telephony systems enabling seamless secure calling between mobile phones and existing landlines, as well as leveraging key features of existing PBX systems such as access to corporate voicemail and conference calling facilities.

When configured with a PSTN Gateway it enables Cellcrypt Mobile to call any telephone on the public telephone network even when the destination phone is not Cellcrypt-secured. The call segment between Cellcrypt Mobile and Cellcrypt Enterprise Gateway is secured, to provide privacy when making mobile calls from untrusted international locations to domestic or trusted destinations.

Cellcrypt Enterprise Gateway works with standard PBX infrastructure so that there is no need to deploy new phones or replace existing equipment and can be integrated with all major providers of PBX technology.

Key Features

- **Extend Private Branch Exchange (PBX) features securely to mobile phones**
  - Call office landlines from mobile phones
  - Access corporate voice mail securely
  - Join conference calls securely
  - Securely call out to any phone on the public telephone network
- **Security**
  - Secures mobile phone calls to and from standard office PBXs
  - Strong end-to-end encryption between Cellcrypt Enterprise Gateway and Cellcrypt Mobile-enabled devices
  - US Government FIPS 140-2 validated (cert number 1310)
- **Simple to use & manage**
  - Incoming secure call announcements and outgoing secure call routed from PBX to Gateway
  - Integrates with standard PBXs and uses existing phone infrastructure
  - Simple to integrate with PBX dial plans
- **Superior performance**
  - High call quality with low latency
  - International calls to mobile phones in 200+ countries
- **Scalable**
  - A single Cellcrypt Enterprise Gateway can support thousands of desk phones

Cellcrypt Enterprise Gateway

Connect securely to your office phone system

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 mobile phones or endpoints. 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).

Cellcrypt's Secure Voice Network

Cellcrypt offers the most flexible yet secure voice architecture available:

- Cellcrypt Enterprise Gateway connects with commonly available mobile phones (e.g. Android™, BlackBerry®, iPhone® and Nokia®) that are secured with Cellcrypt Mobile – anywhere in the world
- Cellcrypt Enterprise Gateway integrates with SIP-based and legacy PBXs and telephony gateways
- Cellcrypt secured mobile phones call other Cellcrypt secured mobile phones
- Cellcrypt secured PBX landlines can call other Cellcrypt secured PBX landlines
- In combination with your PBX, Cellcrypt Enterprise Gateway can route calls to and from office phones or calls out to phones on the PSTN
- Highly flexible through use of DTMF to leverage PBX features

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, ECDH 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 keys.

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.

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

Cellcrypt Enterprise Gateway is made up of Asterisk and the Cellcrypt Gateway product, running on a supported Linux platform.

Supported Platforms

- **PBXs and Telephony Gateways**
  - Integrates with SIP-capable PBXs and Gateways
  - Legacy PBXs and Gateways using SIP (RFC 3261)
- **Operating Requirements**
  - Linux (Redhat Enterprise Server 5.0+; Fedora Core 6.0/8.0+; Centos 5.0+), Asterisk PBX 1.4
  - Extensible using standard channel drivers and 3rd party analogue and digital telephony cards
  - Internet connectivity to Cellcrypt Switch (Ports 443 TCP and 7351 UDP) and connectivity to PBX (Ports depend on PBX configuration)

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