Cellcrypt Private Switch

Create and manage your own secure and private voice-calling network

Cellcrypt Private Switch™ provides complete control of and privacy for your secure voice-calling network.

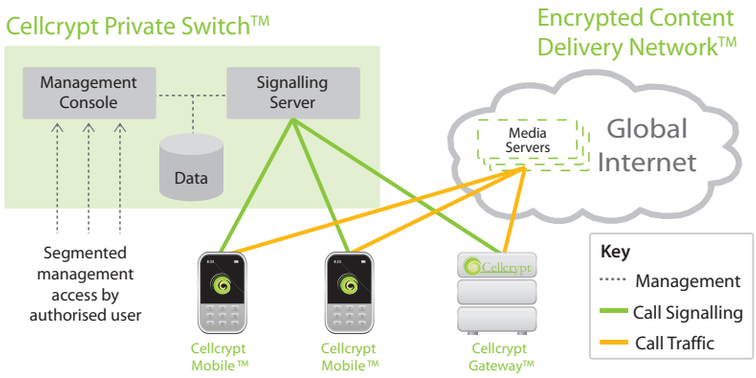
Protecting Valuable Information

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 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 mobile phones – and securely connected to office phone systems – so that you can be assured conversations remain confidential wherever they are.

Cellcrypt Mobile™ and Cellcrypt Enterprise Gateway™ enable secure voice calls between mobile phones, office desk phones or a combination of each. The solution uses end-to-end encryption validated to the FIPS 140-2 standard developed by the US National Institute of Standards and Technology (NIST).



Encrypted Content Delivery Network™

Cellcrypt operates a global network of resilient and secure servers for carrying secure call traffic and optimising call performance beyond that which is available using only the public Internet. It does not participate in the security of the call, neither the trust relationship between callers nor the encryption of the voice call data which has end-to-end encryption.

Additional Privacy for Secure Voice-calling Network

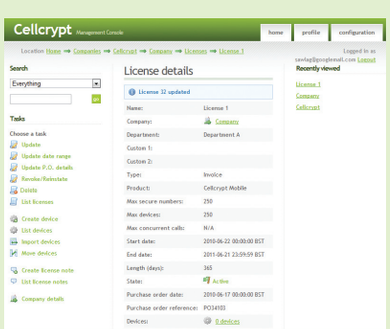
For organisations that require complete infrastructure control for call signalling and user management, Cellcrypt provides enterprise server software, Cellcrypt Private Switch, that installs and operates entirely on customer-defined equipment and is administered via a web-based management console that only customer-authorised users can access. Cellcrypt's Private Switch consists of a Management Console and Signalling Server, enabling organisations to manage and control a completely private network of devices, users and secure numbers.

Key Features

- Secure enterprise software consisting of a Signalling Server and web-based Management Console

- **Signalling Servers**
  - Full, scalable control of user's secure calling network
  - Full control of call signalling and call routing
  - Full control of infrastructure and data
  - Private registration of users and devices
  - Secure call signalling and secure call traffic

- **Performance**
  - Web-based with easy-to-use navigation such as hyperlinks, global search, recently viewed
  - Manages user groups, licenses, devices and secure number plans
  - Multiple items per set (e.g. multiple devices per license, multiple secure numbers per device)
  - Hierarchical user groups with multiple layers of owner, provider and user
  - Role-based access with administrator, support, view and view privileges



Cellcrypt Management Console

Cellcrypt Private Switch

Create and manage your own secure and private voice-calling network

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 Private Secure Voice Network

Cellcrypt offers the most flexible yet secure voice architecture available:

- Cellcrypt secured mobile phones call other Cellcrypt secured mobile phones
- Cellcrypt secured mobile phones call Cellcrypt secured PBXs landlines
- Cellcrypt secured PBX landlines call other Cellcrypt secured PBX landlines
- Different office telephony systems can be securely bridged using Cellcrypt Enterprise Gateway
- In combination with PBXs, Cellcrypt Enterprise Gateway routes calls to and from office phones or calls out to phones on the public telephone network

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.

Supported Platforms

- Linux /x86, running on standard hardware sized according to expected system capacity
- Default ports used:
  - 443 TCP for Signalling Server and Management Console
  - 7351 UDP for Media Server
- IE 7+, Firefox 3+ and Safari 4+ browser access to Management Console
- Optional integration with OpenSSL to provide SSL support on Signalling Server and Management Console
- Reference solutions for resilient configurations with automatic failover are available on request
  - Uses an active/passive pair of signalling servers and an extensible set of media servers
  - Requires additional hardware for SSL termination and automatic fail-over

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