Cellcrypt Secure Conference Service

Protect your information in conference calls

Cellcrypt enables secure access to conference call bridges with encrypted calls from mobile phones, so your team can speak with confidence, wherever they are.

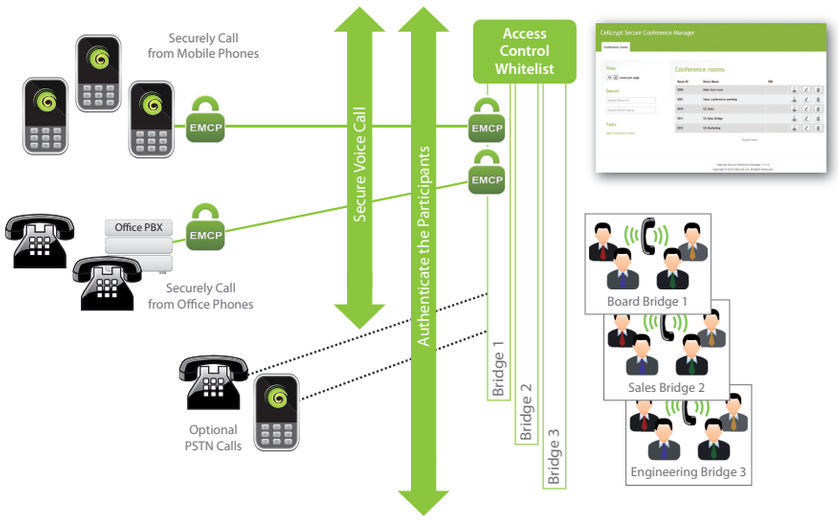
Conference Calls – Mobility and Security

Organisations depend on conference calls to run their daily operations. But as employees become more mobile and the speed of business becomes faster, there is a growing need for people to join conference calls from wherever they are - which often means using their mobile phone either for convenience or out of necessity.

Traditional conference bridges make it difficult to control who is on a call. Long lived PINs are often distributed freely, making conference calls easy to access by unauthorised parties such as ex-employees.

Because conference calls very often contain highly confidential and sensitive information – such as Board and Executive Management Team calls, Intellectual Property discussions, high value business deal talks, crisis management calls or discussions concerning disaster scenarios and national security– organisations need to take steps beyond simple access control to reduce the risk of targeted, malicious attacks. They need to strongly authenticate the calling devices and secure the conversations.

Protecting Conference Calls



Speak with confidence

Cellcrypt Secure Conference Service™ is an easy-to-use solution for extra-secure access and encrypted calling within a secure conference bridge, accessible from mobile phones.

Cellcrypt secure conference calling uses strong cryptographic authentication in combination with pre-defined phone numbers to ensure that only authorised phones can join. The service has an easy-to use web-based management console for setting up any number of bridges with eligible participants defined using a white list policy.

Key Features

- **Security**
  - Strong end-to-end voice call encryption
  - US Government FIPS 140-2 validated (cert number 1310)
  - PIN authorisation
  - Pre-defined caller white lists
  - Strong authentication and encryption for secure access
- **Simplicity & performance**
  - Use direct from Cellcrypt Mobile™ application on popular mobile phones such as Android, BlackBerry, iPhone and Nokia smartphones
  - High call quality with low latency
  - Operates on all wireless data networks including 2G, 3G, Wi-Fi™ and satellite
  - International calling in over 200 countries
- **Secure Conference Features**
  - Secure mobile access via Cellcrypt Mobile, and secure landline access via Cellcrypt Enterprise Gateway™
  - Create and manage private conference bridges through web-based console White lists of eligible callers
  - Access from PSTN
  - Entry / exit announcements
  - Volume adjustment: self / callers
  - Up to 25 callers per bridge, any number of bridges
- **Network Support**
  - Any IP-enabled network, e.g.
    - GSM/CDMA
    - 2G
    - 3G
    - 4G
    - Satellite
    - Wi-Fi™

Cellcrypt Secure Conference Service

Protect your information in conference calls

An optional policy setting enables eligible participants to gain access to the bridge from a standard phone, if required, using a pre-defined phone number and PIN. This allows an administrator to mix unencrypted calls from selected phones over the public telephone network with secure calls from other locations where calling is a concern.

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 devices.

The IP-based solution consists of Cellcrypt Secure Conference Service and a Cellcrypt Mobile application on each participating mobile phone. In an encrypted conference call, each mobile phone has its own dedicated secure connection to the bridge with voice data being encrypted/decrypted at both end points. The service connects all calls together in a single bridge, performing simultaneous encryption/decryption for every call to allow participants to speak to each other in confidence. In addition a bridge can require a user to authenticate themselves with a PIN, which provides 2-factor authentication to access the service.

Cellcrypt 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 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
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