Cellcrypt

Cellcrypt Mobile Solution for BlackBerry Enterprise Server

Speak with Confidence on your cell phone

Cellcrypt Mobile Solution for BlackBerry® Enterprise Server (BES) deploys secure voice calling within Security Policies managed by BES Administrators

Providing 360° Security for BlackBerry Smartphones

Organisations that use BlackBerry Smartphones have invested in the encryption of email, messaging and data to government-level standards. With BlackBerry Enterprise Server organisations have further capitalised on the efficient and secure management and control of devices and policies by IT Administrators.

In contrast, government-grade security and centrally controlled management of voice calling on Smartphones often is not implemented to adequately protect against the threat of mobile phone interception. The risk of interception is increasing as equipment is becoming cheaper and more accessible: in 2010 the cost of mobile phone interception was significantly reduced when 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 publicly demonstrating interception equipment that is readily available for under $2000[2].

With Cellcrypt Mobile for BlackBerry, voice calls are encrypted on BlackBerry Smartphones so that the device, data and voice is secured to government-grade standards to provide 360° security of all mobile communications

Deployed and Managed by BlackBerry Enterprise Server

Cellcrypt Mobile™ for BlackBerry is a downloadable software application that makes secure calling as easy as making a normal call using the IP data network to deliver unparalleled voice quality, low latency and global calling capability – all delivered to government-level security standards. It is deployed and managed entirely through the BlackBerry Enterprise Server using pre-set policies, meaning that the secure voice calling capability can be deployed under full control of an organisation's IT and Security Policies to any employee anywhere in the world in minutes by the BlackBerry Enterprise Server Administrator.

Cellcrypt Mobile connects seamlessly to PBXs infrastructure via a server-based encryption endpoint (Cellcrypt Enterprise Gateway™) that integrates with PBXs to enable organisations to maintain PBX call recording solutions, dial plans and DTMF sequences as well as support PBX extension numbers, voicemail and conference calling capabilities.

Cellcrypt's Technology

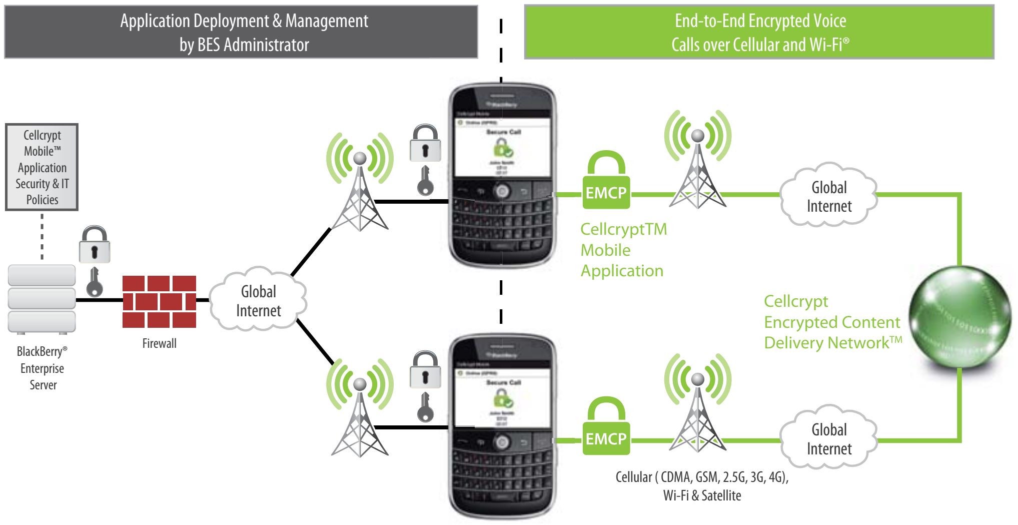
Cellcrypt's advanced solution leads the industry in delivering multi-layered security to establish a high-performance encrypted voice call between trusted wireless devices. It utilises Encrypted Mobile Content Protocol (EMCP), a set of standards-based protocols for optimising delivery of encrypted real-time content between cell 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).

Key Features

- **Security**
  - Strong end-to-end encryption
  - US Government FIPS 140-2 compliant
- **Management**
  - Deployed and controlled entirely through BES
  - Integrates to PBXs for call recording, voicemail and conference calling support
- **Key Benefits**
  - Easy to install, manage and push encrypted voice capability to any user globally
  - Secure deployment under control of IT Policies and Administrator
  - Enables personnel to talk about emails and documents they have sent & received
  - Provides security of executives' travel and logistical information which can be exploited, especially when travelling abroad, for kidnap, extortion and ransom
  - Low-cost calling over Wi-Fi® reduces bills, especially when roaming
- **Network Support**
  - Any IP-enabled network, e.g.
    - GSM/CDMA
    - 2G
    - 3G
    - 4G
    - Satellite
    - Wi-Fi™

Cellcrypt Mobile Solution for BlackBerry Enterprise Server

Speak with confidence on your cell phone


Application Deployment & Management by BES Administrator
End-to-End Encrypted Voice Calls over Cellular and Wi-Fi®
Cellcrypt Mobile™ Application Security & IT Policies
BlackBerry® Enterprise Server
Firewall
Global Internet
EMCP
CellcryptTM Mobile Application
Global Internet
Cellcrypt Encrypted Content Delivery Network™
EMCP
Global Internet
Cellular (CDMA, GSM, 2.5G, 3G, 4G), Wi-Fi & Satellite

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

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

BES.A4.V2.3