Cellcrypt

Cellcrypt Mobile Baseline

Speak with confidence on your mobile phone

Cellcrypt Mobile Baseline™ is a CAPS approved IL3/RESTRICTED encrypted voice software solution for BlackBerry® smartphones.

Protecting UK Government Information

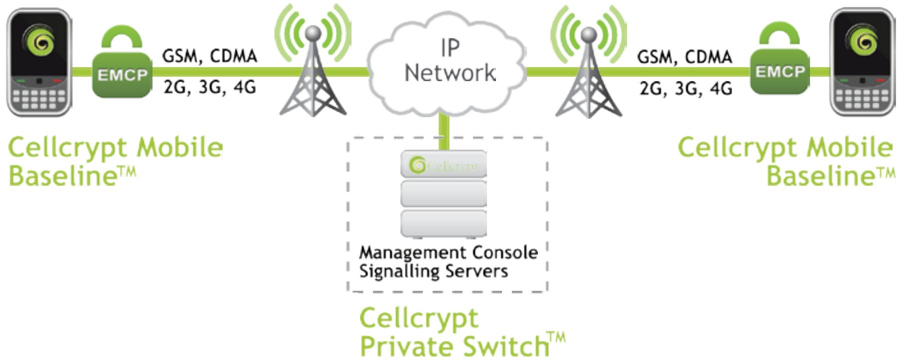
Cellcrypt Mobile Baseline provides end-to-end voice call encryption on commercially available off-the-shelf BlackBerry smartphones. It is an easy-to-use software application that makes secure calling as easy as making a normal mobile phone call and uses the IP (Internet Protocol) data channel of mobile (2G, 3G, and 4G) networks.

Cellcrypt Mobile Baseline has been CAPS approved to protect information up to and including the classification level RESTRICTED (Impact Level 3) when configured in accordance with CESG Security Procedures. CAPS (CESG Assisted Products Service) is the UK Cryptographic Evaluation Service run by CESG, the UK Government's National Technical Authority for Information Assurance.

The system uses a decentralised public key management architecture that does not require CESG key material. Ephemeral keys are generated and held only within the Cellcrypt Mobile endpoints.

Operation of the solution relies on management and switching components that must be hosted in a secure environment suitable for IL3/RESTRICTED data.

End-to-end security on commercial off-the-shelf BlackBerry smartphones



Easy to Use, Deploy and Manage

As a software-only solution, Cellcrypt Mobile Baseline is easy to use, manage and deploy: a secure voice capability can be provided to users over-the-air anywhere in the world in minutes under the full control of the BlackBerry Enterprise Server administrator.

Newly provisioned users can securely communicate directly with each other as soon as they have installed the application. Users can easily change handsets and/or SIM cards. Access to the service can be revoked remotely in seconds.

Key Features

- **Security**
  - CESG CAPS approved
  - End-to-end encryption
  - Designed to work with CESG policy for mobile at IL3/RESTRICTED
- **Simplicity**
  - Runs on COTS BlackBerry smartphones
  - No specialist equipment required
  - Intuitive user experience
  - Managed by BlackBerry Enterprise Server (BES)
- **Performance**
  - High call quality with low latency
  - Operates on appropriate data-capable wireless networks
  - International calling in over 200 countries
- **Supported Devices/Networks**
  - Approved BlackBerry RIM OS5 & OS7 devices
  - Any IP-enabled network, e.g.GSM/CDMA, 2G, 3G and 4G

Cellcrypt Mobile Baseline

Speak with confidence on your mobile phone

Cellcrypt's Technology

Cellcrypt's solution is an industry leader in delivering a software-only solution to establish a high-performance encrypted voice call between trusted smartphones, using an intuitive interface. It is designed to provide encrypted voice calls in challenging mobile environments where network factors are significant. The service maintains high performance voice call attributes such as fast call set up, high voice quality and low latency. It does this by using Encrypted Mobile Content Protocol™ (EMCP) over the IP data channel.

Encrypted Mobile Content Protocol

EMCP covers three areas:

- High-speed mechanisms to establish encrypted data streams in real-time using standard encryption algorithms
- Establishment of a secure end-to-end channel between mobile handsets, and authentication and routing of encrypted data streams between them without the requirement for a key server
- Mechanisms that ensure high performance data stream delivery over low bandwidths

Secure Private Voice Network

Government organisations can operate their own secure private voice network, and manage and control a private set of devices, users and secure numbers within their own network infrastructure by deploying a Cellcrypt Private Switch™.

The Cellcrypt Private Switch - consisting of a Management Console and Signalling Server - validates software licenses, sets up and routes calls. Importantly it does not participate in the end-to-end security of the call which is managed directly between the endpoints and provides end-to-end encryption between those endpoints.

Cryptography

Cellcrypt uses standard encryption technologies including:

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

ECDSA is used for authentication. The key pairs are generated on the phone during the installation and are unique to each phone. Ephemeral session keys are generated per call to ensure forward secrecy. The ECDH algorithm is used for key exchange. The session key is only valid for one phone call and securely destroyed after use. AES is used to symmetrically encrypt the voice stream.

About Cellcrypt

Cellcrypt is a leading provider of encrypted voice calling on commercial off-the-shelf mobile phones including Android, BlackBerry, iPhone and Nokia smartphones. It enables secure, interoperable calling between a broad selection of popular mobile phones and interfaces to PBXs over IP-enabled networks, including Wi-Fi™.

Founded in 2005 in the UK, 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
Cellcrypt FZE
PO Box 38255
Dubai
UAE
Tel: +971 (0)4454 1271

Email: info@cellcrypt.com
Web: www.cellcrypt.com