Cellcrypt®
VOICE GATEWAY

Secure, Encrypted Calls Between Land Lines and a Mobile Workforce

Organizations are struggling to provide the seemless connectivity they get from their office phones systems to an increasingly mobile workforce. Moreover, businesses need to control and significantly reduce the substantial costs of mobile communications.

Smart businesses are also looking for communication solutions that allow them to talk to their customers, on their mobile devices, wherever they are; safely, securely and at a reasonable cost.

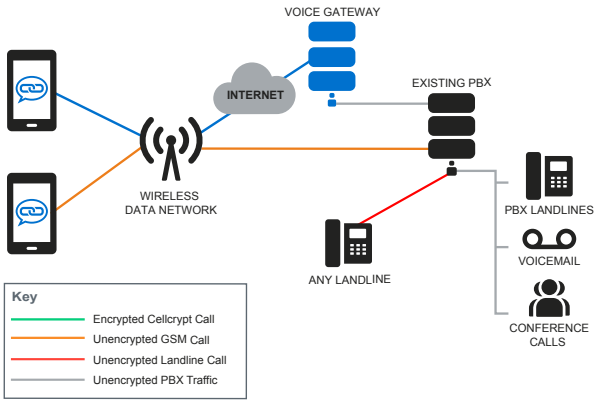
Making the switch to VoIP, as a solution to this problem, is attractive, but how can this be acheived securely, with an existing PBX infrastructure?

Create a Secure VoIP to PBX Connection

The Cellcrypt Secure Voice Gateway provides an encrypted VoIP channel that integrates seamlessly with any existing digital PBX infrastructure.

This allows organizations to extend the benefits of their existing PBX features, including voicemail and conference calling, to mobile users with the reduced costs of VoIP and the strong encryption provided by Cellcrypt.

- Cellcrypt Voice Gateway integrates with SIP-based and legacy PBXs and telephony gateways
- Cellcrypt secured mobile phones can call other Cellcrypt secured mobile phones
- Cellcrypt secured PBX landlines can call other Cellcrypt secured PBX landlines
- In combination with your PBX, the Voice 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



- Securely connect to the company PBX to reach offices, customers and employees
- Access PBX infrastructure, including conferencing and voicemail, securely from anywhere in the world
- Dramatically reduce calling costs by eliminating international roaming and long distance charges
- Protection from data interception using military-grade encryption on VoIP calls between mobile devices and secure PBXs

Secure, Cost-Effective Access To Your Existing Phone System

The Cellcrypt Voice Gateway interfaces to a wide-range of digital PBXs so that you can leverage and maximize the benefits of your existing infrastructure without the need for a costly rip/replace strategy and by utilizing Cellcrypt's secure Voice over IP (VoIP) network, international and long-distance call costs are eliminated.

When configured with a PBX the Cellcrypt Voice Gateway allows any Cellcrypt user to make calls to any non-Cellcrypt-secured phone connected to the PBX.

The call segment between the Cellcrypt user and the Cellcrypt Voice Gateway is encrypted providing privacy and security when making calls from potentially untrusted and/or international locations to trusted and/or domestic locations.

Operating Requirements

1. Linux (Debian / Ubuntu)
2. Extensible using standard channel drivers and 3rd party analogue and digital telephony cards
3. Internet connectivity to Cellcrypt Private Switch and connectivity to PBX

Cellcrypt®
TRUSTED COMMUNICATIONS

Military-Grade Encryption for Secure Communication

Cellcrypt provides high grade, end-to-end encryption for secure voice calls messages and file transfers between trusted mobile devices.

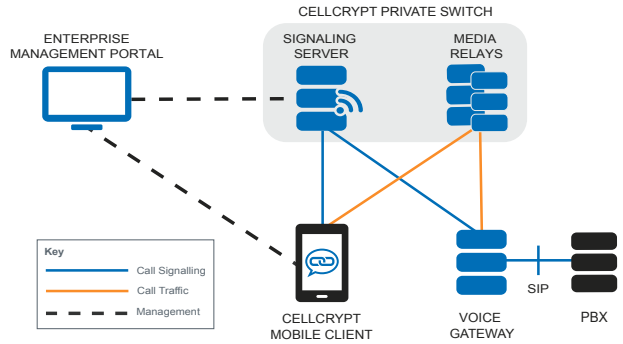
For protection of voice calls, instant messages and content, the Encrypted Mobile Content Protocol™ (EMCP) optimizes delivery of encrypted content in real-time, even across low-bandwidth wireless networks.

Cellcrypt uses standard encryption technologies including:

- Advanced Encryption Standard (AES) for symmetric encryption
- 384-bit Elliptic Curve Cryptography for Authentication
- Elliptic Curve Diffie-Hellman (ECDH) for key agreement
- Secure Hash Algorithm (SHA) for message digest

Cellcrypt's Dual Cipher system uses double-wrapping for added security. For example, voice calls are first encrypted using RC4 with a 384-bit key and then encrypted again using AES with a 256-bit key.

CELLCRYPT® ENCRYPTED CONTENT DELIVERY NETWORK



Cryptography

Key Generation

- Entropy collected continuously from hardware sources e.g. motion sensor, mic and OS sources e.g. /dev/urandom
- Long term ECC keys generated & stored in application's secure database
- No manufactured/generated key material is needed prior to use of the system

Voice Call Authentication

- Secure data exchange in two stages
- End-to-end standards-based key establishment providing mutual authentication, Perfect Forward Secrecy (PFS) and unique keys per-session
  - NIST SP800-56A C(2,2) Full Unified Model with Bi-lateral Key Confirmation
  - Authentication using NIST approved ECC curve P-384

Message Authentication

- End-to-end standards-based key establishment with mutual authentication
  - NIST SP800-56A C(1,2) One-Pass Unified Model
  - Public key fingerprint displayed in message dialog and contact details for vocal confirmation

Symmetric Cryptography

- Dual ciphers - RC4 with 384-bit key and AES-CTR with 256-bit key
  - FIPS SP 800-38 – AES in CTR mode and AES in GCM mode (rev D)

NIST FIPS 140-2 Level 1 Certified

- Cellcrypt is certified to the FIPS 140-2 standard, approved by the US National Institute of Standards & Technology (NIST) (CERTIFICATE # 2575)

Cellcrypt is the complete solution for trusted mobile communications, providing secure, real-time messaging, voice/conference calling and secure file transfer, all protected by strong, authenticated, end-to-end encryption.

Combining military-grade security with the ease of use of a consumer app, Cellcrypt requires no user training/configuration, ensuring fast and easy deployment, user acceptance and adoption across your organization.

With Cellcrypt you can trust that your confidential communications remain that way.

DANMIK AGENCIES
email: info@danmik.com
www.cellcrypt.com.au