seecrypt
COMMUNICATE IN CONFIDENCE

VOICE GATEWAY

Secure calls between mobiles and your office phone system

Organizations are struggling to provide the seamless 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.

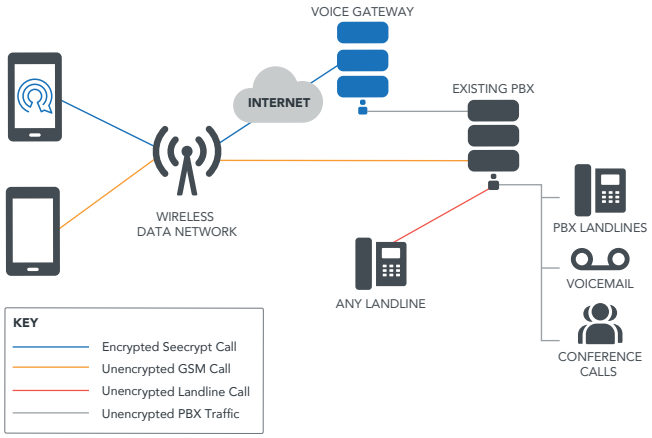
Making the switch to VoIP, as a solution to this problem, is attractive, but how can this be achieved securely, with an existing PBX infrastructure?

Create a Secure VoIP to PBX Connection

The Seecrypt Voice Gateway provides an encrypted VoIP channel to seamlessly integrate with your existing digital PBX infrastructure.

Allowing organizations to extend their existing PBX features, with benefits including voicemail and conference calling, to mobile users. This increased functionality is accompanied by the cost savings associated with VoIP, and the security and strong encryption provided by Seecrypt.

- SIP-based and legacy PBXs and telephony gateways integrate fully with Seecrypt Voice Gateway
- Secure calling between mobiles using Seecrypt
- Secure calling between Seecrypt PBX landlines
- Voice Gateway combines with your PBX, to allow routing of calls to and from office phones or to phones on the PSTN
- High flexibility through use of DTMF to leverage PBX features



Reach offices, customers and employees through a secure connection to the company PBX

Extend your PBX infrastructure, with voicemail and conferencing, securely from anywhere in the world

Eliminate international roaming and long distance charges to dramatically reduce calling costs

Military-grade encryption protects from data interception on VoIP calls between the secure PBX and mobile devices

Secure, Cost-Effective Access To Your Existing Phone System

The Seecrypt 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.

- Bring Voice of IP (VoIP) capabilities to your legacy PBX, transforming its functionality and extending the infrastructure lifetime
- Gain the cost benefits of eliminating international and long-distance call costs from your landlines/office phones to mobile
- Enable secure, end-to-end encryption calling to your mobile workforce, wherever they are in the world
- Extend the security and functionality of your existing PBX to your entire network, including conference calling and voicemail

OPERATING REQUIREMENTS

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

seecrypt
COMMUNICATE IN CONFIDENCE

ENCRYPTION

Military-Grade Encryption for Secure Communication

Seecrypt provides secure voice calls, messages and file transfers between trusted mobile devices via high grade, multi-layered encryption.

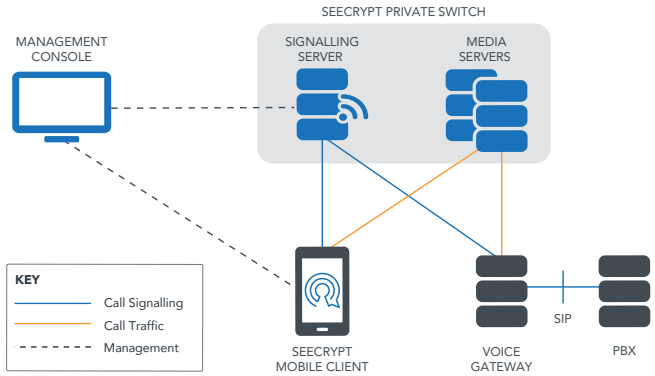
Protection of all communication and content is guaranteed by the Encrypted Mobile Content Protocol™ (EMCP), with real-time optimized delivery of encrypted content, even across low-bandwidth wireless networks.

Seecrypt 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

Seecrypt's Dual Cipher system uses double-wrapping for added security. Voice calls, for example, are first encrypted using RC4 with a 384-bit key, followed by a second encryption again using AES with a 256-bit key.

SEECRYPT® 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)

Seecrypt is the global solution for trusted mobile communications, providing private, real-time messaging, voice/conference calling along with file sharing and transfer. Protected by leading-edge, authenticated, end-to-end encryption.

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

With Seecrypt you can trust that your confidential mobile communications remain confidential.

CSG
COMMUNICATION SECURITY GROUP

www.seecrypt.com

email: info@seecrypt.com