seecrypt
COMMUNICATE IN CONFIDENCE

PRIVATE SWITCH

Create your own, private, voice and messaging service

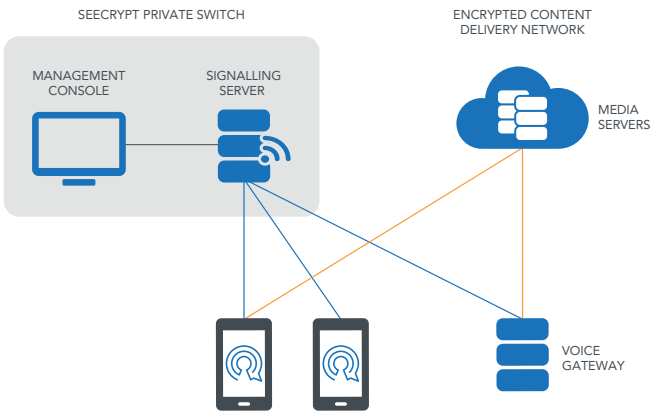
Enable total security and take control of your organization's mobile communications.

Seecrypt's Private Switch is the core of control for Seecrypt, administered via a web-based management console. Access is restricted to authorized users only.

Private Switch manages users; call signalling; call control and media communications and authenticates/authorizes every interaction within the network.

Seecrypt Private Switch is designed to be used with the Encrypted Content Delivery Network – our global network of secure and resilient media servers designed for carrying call and message traffic.

ENCRYPTED CONTENT DELIVERY NETWORK™ (ECDN)



PRIVATE SWITCH INFRASTRUCTURE

Signaling Server

- Processes authentication and call set-up for all clients
- Includes Seecrypt's Enterprise Management Portal for management and control of all users and devices on the Seecrypt network

Media Server

- Routes encrypted packets between two devices involved in media session
- Media Relays operate outside the Seecrypt Network and are deployed in multiple global locations to reduce latency in media sessions
- The media relays record no user identifiable information or metadata regarding any media session
- The system ensures packets are correctly delivered, even on poorly performing networks

Management Console

- Web-based administration with dashboards
- Detailed reporting
- User Management

ON PREMISE OR IN THE CLOUD

We offer a choice of installations, with the Seecrypt Secure Switch infrastructure installed and operated fully on-premise within your own environment. Alternatively, the Secure Switch can be hosted as a cloud-based solution for reduced infrastructure and running costs.

CSG
COMMUNICATION SECURITY GROUP

www.seecrypt.com

email: info@seecrypt.com

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.

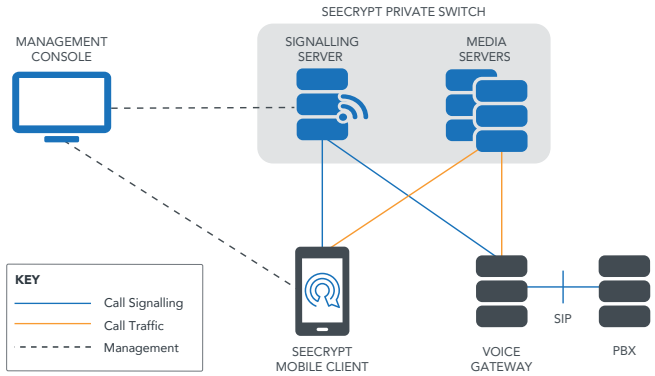
Protection of all communication and content is guaranteed by the Encrypted Mobile Content Protocol™ (EMCP), with real-time optimized delivery of encrypted content, even across low-bandwidth wireless networks.

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