

# CONFERENCE CALLING

Instant access to secure,  
encrypted mobile conferencing



Group calling can be set up instantly from your contacts list in seconds, just like a regular call



Schedule mobile and desktop conference calling with automatic email invites, and no need for third-party administrators or passwords



Secure, end-to-end encryption combines with call moderating, mute and eject options for the call initiator



Seecrypt Conference Calling can combine with Seecrypt Voice Gateway via your PBX to extend calling to non-Seecrypt users

## End-to-End Encryption

Advanced cryptographic techniques ensure the privacy of conference calling even for mobile users operating within hostile environments.

## Secure Scheduling and Call Controls

In addition to end-to-end encryption, the Seecrypt Conference Calling web UI ensures that your business can enjoy secure, authenticated conference calling, safe in the knowledge that the right people are on the line. Call initiator or administrators have a full attendee list, and can easily invite new participants, mute and even eject callers if the need arises.

## Forget Passwords, PINs and Dial-ins

Ensuring all participants have the correct information to join a call is major inconvenience with normal conference calling. Pins, passwords and international dial-in numbers can slow everything down, incur expensive long-distance charges, and even prevent crucial participants from joining calls.

With just one touch, Seecrypt Conferencing enables participants to join a cost-effective, secure VoIP conference call, already fully authenticated and ready to contribute.

Seecrypt Conference Calling is a cost-effective way to take the complication out of group calls and scheduled tele-conferencing. Make secure, encrypted calls whenever you want, from your mobile or desktop, leveraging your existing infrastructure for seamless, immediate collaboration.

Secure group calls can be set up instantly from your contacts on mobile or desktop. Scheduled conferencing offers simple, straight forward calling and email invites, eliminating the need to arrange through a third party, or issue passwords. The call initiator can retain full control with a web UI that provides a complete list of attendees invited and present, plus mute and eject options.

An open bridge that can be 'always on' provides the organization with instant collaboration and messaging functions with zero set up time.

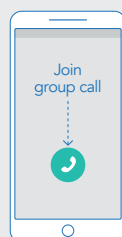
When combined with Voice Gateway and directed through your organization's existing PBX, Conference Calling can even be extended via mobile, desktop or landline to non-Seecrypt users.

Hosting can be provided via the cloud, through on-site servers, or on a hybrid of the two, as best suits the organization.

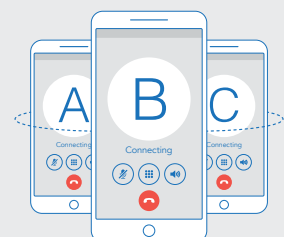
## INSTANT GROUP CALLING – Start a Seecrypt Conference Call from your smart phone at any time.



Select participants from your phone's contacts list



Press call and the bridge is created, connecting you directly



The other participants get a message to join the call

# 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.

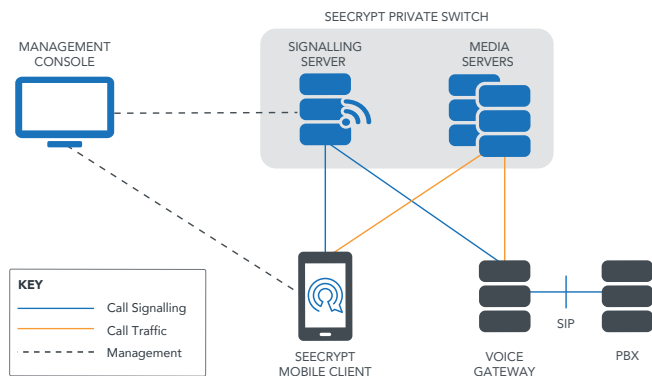
Protection of all communication and content is guaranteed by the Encrypted Mobile Content Protocol™ (EMCP), with real-time optimized delivery of encrypted content, even across low-bandwidth wireless networks.

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.



[www.seecrypt.com](http://www.seecrypt.com)

email: [info@seecrypt.com](mailto:info@seecrypt.com)