In-Confidence

Next generation encrypted voice, messaging and conference for iPhone & iPad

- **Secure Voice**
- **Secure Messaging**
- **Secure Multi-Party Conference**
- **Military Grade Encryption**

TRIPLE LAYER 3 X 256 BIT SECURE STRONG ENCRYPTION TOP SECRET

Works with iPhone

No Compromise Encrypted Telephony

In-Confidence is SecureGSM's next generation product designed to deliver our famous triple-layer encryption to Internet Telephony (Voice over IP - VoIP) communications.

In-Confidence boasts an unparalleled level of security combined with state-of-the art, echo-free audio quality using superior quality audio engine components. But what truly sets *In-Confidence* apart from the competition is that it is the only dedicated multi-party conferencing product with triple layer encryption capabilities.

These unique features combine to make *In-Confidence* the most user-friendly encrypted telephony application with a no-compromise security model.

Unmatched Feature Set

- Unprecedented security, with intuitive ease of use
- SecureGSM's famous triple cipher encryption module (true military grade security)
- Crystal clear, echo-free voice calls
- Speakerphone compatible
- Point-to-point encrypted voice calls
- Multi-party encrypted conferencing
- Encrypted, verified multi-language enabled messaging
- Integrated contacts manager with search functionality
- Intuitive, easy to use graphical user interface
- Closed Group capabilities
- Robust party verification procedures
- Advanced program protection, designed to withstand penetration of code intruders and malicious reverse engineering

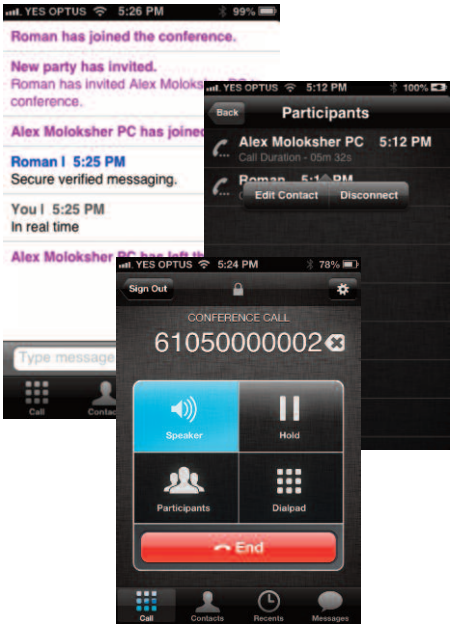
TRIPLE LAYER 3 X 256 BIT SECURE STRONG ENCRYPTION TOP SECRET

Works with iPhone

Advanced Code Potection

Designed to withstand penetration of code intruders and malicious reverse engineering, SecureGSM™ SenTnel™ integrity verification module and SecureGSM™ Signature Verification Tool (SVT) designed to ensure that your product is a genuine SecureGSM security product that has not been compromised in any way whatsoever.

Multi-party Encrypted Conference



Designed to be an essential collaboration tool from the outset, *In-Confidence* features fully encrypted multi-party conference capabilities, a first in the industry.

All standard features work in a multi-party conference. Of course the conference is fully encrypted and all messages are verified for delivery.

Secure, Verified Messaging

Sometimes, relaying information by voice is not viable or even desirable. For this very reason, *In-Confidence* features a fully secured, verified messaging engine which is active during every secure call or conference.

- Confirmation routines clearly identify sent, received and non-deliverable messages.
- Integrity verification routines ensure that the received message is the same as the sent message.
- At no time are you unsure of whether or not the other party has received your message.
- Convenient way to transmit passwords, numbers or any other information which may be problematic to understand by voice.
- Where listening devices are suspected a whole conversation can be conducted using the messaging module.
- Simultaneous secure voice and secure messaging.

Strong Encryption

$$y_S = \lambda(x_1 - x_S) - y_1$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P_1 \neq \\ 3x_1^2 + a \end{cases}$$

There is a reason why SecureGSM coined the term "Military Grade Encryption" back in 2005. We provide an unprecedented level of protection in all our security products. To this day, our products are still the only ones on the market to feature triple cipher cryptography.

Today, of course everyone claims "Military Grade Encryption". The difference is, with SecureGSM products you are assured of the quality of this statement. We don't just use it as a marketing term, we mean it.

- Robust, triple cipher (3 x 256 bit), cascading encryption based on AES, Twofish and Serpent ciphers. Any one of these encryption algorithms is considered unbreakable by today's standards and the triple layer ensures that encrypted data is future proof.
- If any one of the encryption algorithms is broken, or found flawed in the future, it is not possible to obtain data to decrypt or compromise the remaining layers or chains.
- Robust, high performance, asymmetric key generation engine. Private and public keys are generated per session and subsequently destroyed (unrecoverable) upon termination of call.
- Calling party identity verification procedures as protection from "man in the middle" attack and comprehensive procedures to ensure keys or foreign data have not been injected or substituted by a third party.
- Triple ECDH - Elliptic Curves Diffie-Hellman (3 x 571 bit)* Public Key Infrastructure.
- Unique Party Authentication Module.

**571-bit ECDH is currently equivalent in security to 15,360-bit RSA/DH/DSA (based on table 1, RFC 5349 standard; http://tools.ietf.org/html/rfc5349). Therefore, SecureGSM's triple ECDH is approximately equivalent to 3 x 15,360-bit = 46,080-bit RSA/DH/DSA.*

Applications

Applications for *In-Confidence* are many and varied. Just one look at the headlines is all you need to see that security is paramount in today's world of convergent communications.

SecureGSM manufactures products for industries and markets where security is of paramount importance such as:

- Mining and Exploration
- Banking and Finance
- Trading and Exchange
- Research & Development
- Legal, Accounting and Medical
- Automotive and General Manufacturing
- Large Enterprise & SME
- Governmental, Security and Military applications
- Many more where security of information is paramount

Reliable Telephony

A reliable Internet Telephony Service is bundled together with the *In-Confidence* application to ensure that you never miss an important call. Of course, it is strictly a pass through service – no encryption/decryption ever happens at the switch.

More Information

Further, more detailed information both technical and non-technical is available on SecureGSM's extensive Web site at www.securegsm.com.

Of course, you may also contact us by telephone or email. We will be glad to discuss how we can help you secure your telephony from eavesdropping and interception.

Under the hood

At SecureGSM we believe that security should be as transparent as possible. All our products are designed to be easy to use and no security knowledge is ever expected from the user.

Under the hood however, extremely complex routines, advanced mathematics and unique algorithms all contribute to rock solid stability and true Military Grade encryption.

System requirements

Compatible Handsets:
Apple iPhone® 3GS*, 4, 4S, 5

Network connection:
(3G/4G/LTE/WiFi/Satellite BGAN)
Broadband Internet connection with 50Kbit/sec uplink and 50Kbit/sec downlink minimum per conference participant.

Network protocol:

UDP, ICMP Type 8 and Type 0 network protocols.

secureGSM™
Securing the future of communication

Level 1, 240 Chapel Street, Prahran VIC 3181, Melbourne Australia
Tel: +613 9510 4955 Skype: SecureGSM Email: info@securegsm.com Web: www.securegsm.com