DENCRYPT TALK
ENCRYPTED MOBILE COMMUNICATION

Dencrypt Talk protects your smartphone conversations with state-of-the-art Dynamic Encryption – the best protection against non-secure digital infrastructure like Wi-Fi hotspots, mobile networks, satellite links etc. The user-friendly app requires no special hardware.

DENCRYPT TALK OFFERS:

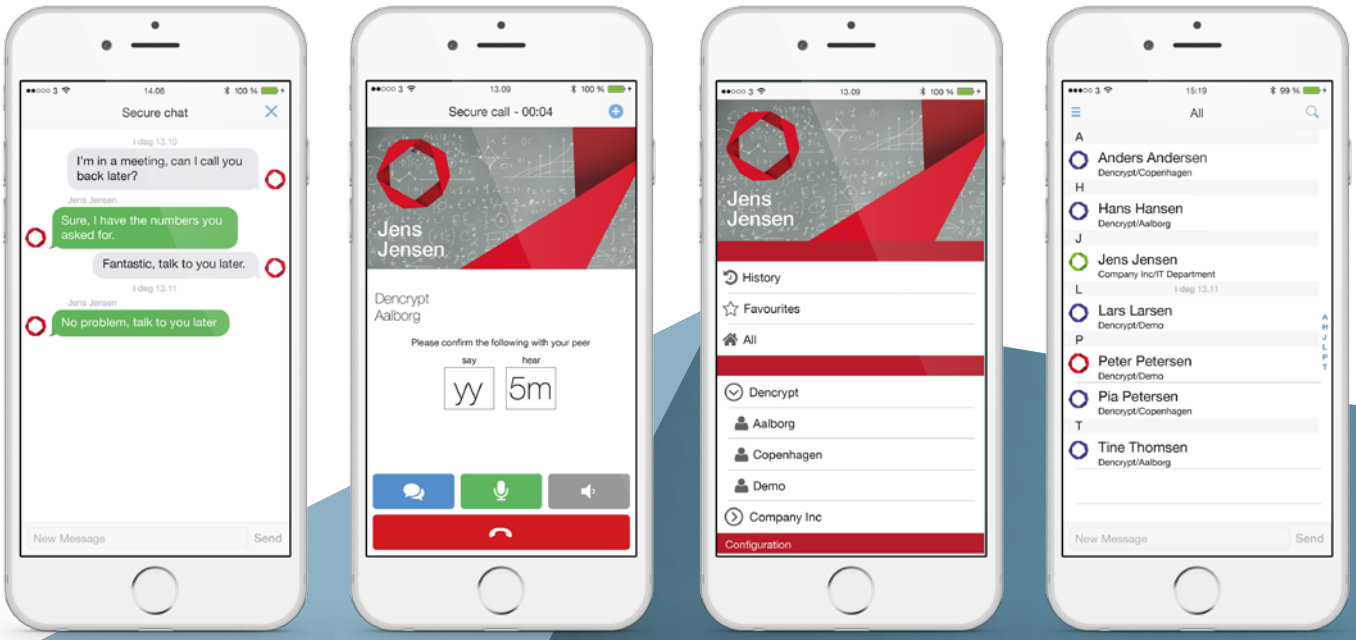
DYNAMIC ENCRYPTION

USER-FRIENDLY OPERATION

PROTECTION OF SMARTPHONE CONVERSATIONS

FEATURE SET

- End-to-end encrypted voice calls via Voice over IP (VoIP)
- Encrypted live chat
- Encrypted group call
- Secure call setup via a dedicated SIP server
- iOS CallKit integration
- High audio quality
- Secure individual phone book
- Centrally managed
- Pushed seamlessly to user devices
- Supports individual groups settings
- Individual ring tones
- In-call functionality: mute, speaker
- Seamless over-the-air SW updates
- Connectivity on all cellular and wireless networks, including:
  - GSM/EDGE, WCDMA,HSPA, LTE, Wi-Fi
- Major mobile platforms supported
- iOS and Android
- Windows phone (on request)
- Common Criteria certified (ISO 15408)



Version 1.1

DENCRYPT SECURE TALK
TECHNICAL SPECIFICATIONS

Voice & data encryption
Secure end-to-end encrypted voice communication and chat using Dynamic Encryption, ensures that each call session is encrypted with a randomly chosen algorithm and a randomly chosen key.

- Dynamic encryption of voice data implemented as multiple layers of encryption optimized for voice data over the SRTP protocol:
  - 2 x 128-bit whitening keys as an additional layer to a standard AES-256 encryption.
  - 128-bit key dynamic encryption for defining an additional AES round with randomly chosen S-boxes.
  - Patent pending: PCT/EP2012/071314.
- 3072 bit Diffie-Hellman function for key exchange over the zRTP protocol.
- SAS: four-letter readout based on key authentication .
- Encryption key and algorithm are established at call setup and deleted as soon as call is terminated.
- Random number generation using a Yarrow algorithm on iOS.

Two-way authentication
Client and server authentication and registration for call setup and user account management:

- SIP Secure + TLS1.2 using AES-256-GCM for data protection and ECDHE-RSA for key exchange using a 4096 bit certificate for server authentication and a 3072 bit certificate for client authentication.

Connectivity
Voice-over-IP calls and chat over all cellular, wireless and satellite networks, including GSM/EDGE, WCDMA/HSPA, LTE/LTE-A, Wi-Fi.

Audio
- Adaptive audio quality based on current network conditions.
- Constant bit-rate SPEEX voice codec for optimal security and voice quality.
- Polyphonic ringtones.

Performance
- Same as or better voice quality than non-encrypted voice-over-IP calls. Encryption does not introduce an audible delay or voice quality degradation.
- Fast call setup time and high reliability.
- iOS CallKit integration for improved usability.

Supported platforms
- iOS 10.0 and later.
- Android 4.x (Jelly Bean) and later.

Local Dencrypt Server System
- The Dencrypt Server System (required for Dencrypt Talk) can either be installed and operated locally or used as a hosted service managed by Dencrypt.

Dencrypt A/S
Arnold Nielsens Boulevard 72-74, 1. Sal
2650 Hvidovre
DENMARK

+45 7211 7911
info@dencrypt.dk
www.dencrypt.dk

Version 1.1