

# DENCRYPT TALK

## ENCRYPTED MOBILE COMMUNICATION

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

### DENCRYPT TALK OFFERS:



**ALSO USED BY  
MANAGEMENT**



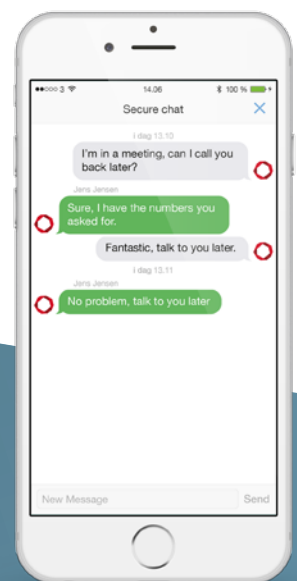
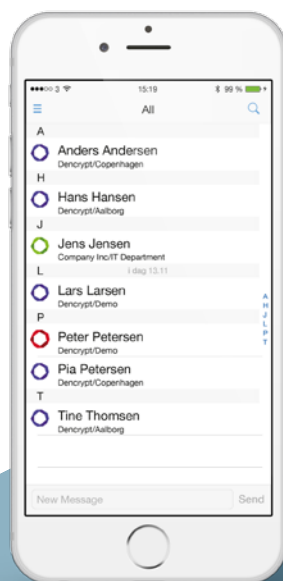
**SERVER IN-HOUSE OR  
CLOUD-BASED**



**DYNAMIC ENCRYPTION**

### FEATURE SET

- » Dynamic Encryption + AES-256
- » 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
- » High audio quality
- » Secure individual phone book
- » Centrally managed
- » Supports individual groups settings
- » Individual ring tones
- » Seamless over-the-air SW updates
- » Connectivity on all cellular and wireless networks, including:
  - » 3G/4G/LTE, GPRS, Wi-Fi
- » iOS and Android
- » Common Criteria certified (ISO 15408)



# DENCRYPT 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 randomly chosen keys.

- » 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.
- » All key material is generated with Cryptographically Secure Pseudorandom Number Generators.

### 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.

### 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 3G/4G/LTE/WIFI, GPRS.

### 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.

### Supported platforms

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

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

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

ENCRYPTION  
USED BY NATO &  
THE DANISH DEFENCE

