ENCRYPTION USED BY NATO & THE DANISH DEFENCE

COMMON CRITERIA CERTIFIED

DENCRYPT

DENCRYPT TALK

Encrypted Mobile Communication

Dencrypt Talk protects your smartphone conversations with state-of-the-art Dynamic Encryption on non-secure digital infrastructure such as WiFi hotspots, mobile networks and satellite links. Dencrypt Talk is a Common Criteria certified, user-friendly smartphone application delivered from Appstore or a mobile device management system.

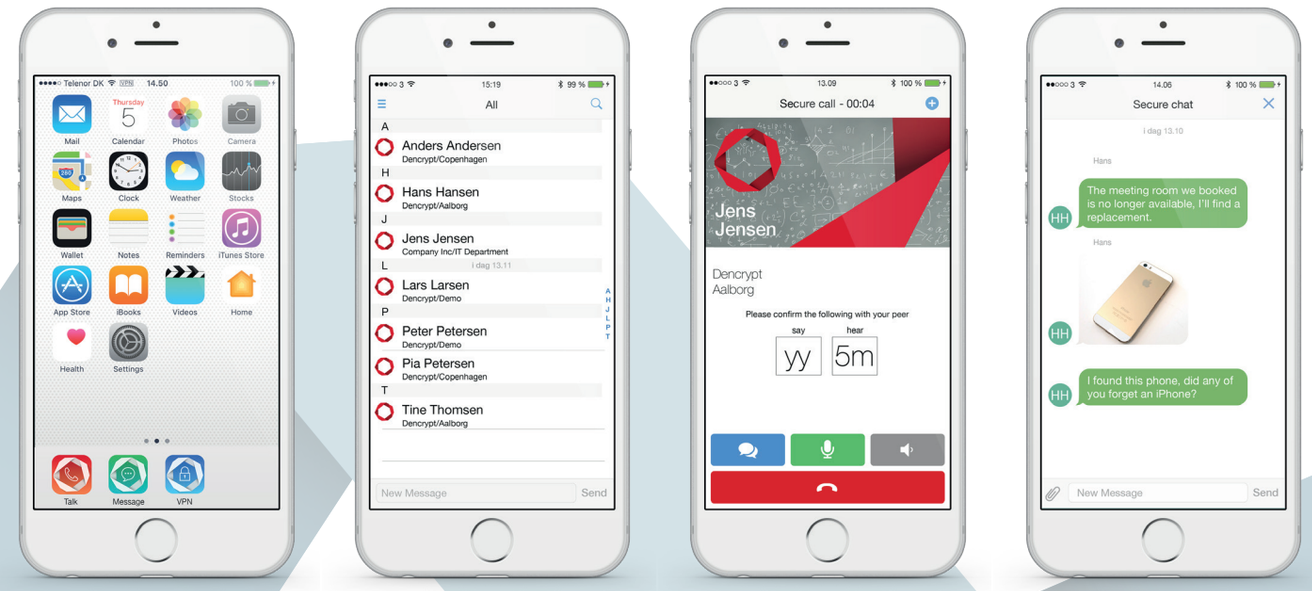
Dynamic Encryption

User-friendly

Certified and Accredited

Feature Set

- Dynamic Encryption + AES-256
- End-to-end encryption
- Perfect Forward Secrecy
- Encrypted voice calls over VoIP
- Encrypted live chat
- High audio quality
- Secure phonebook:
  - Centrally managed
  - Individual call groups
- Secure provisioning
- Connectivity on all cellular and wireless networks
- Mutual authenticated connection.
- Common Criteria certified (EAL4+)
- iOS and Android platforms



DENCRYPT Arnold Nielsens Boulevard 72 | DK-2650 Hvidovre | Phone: +45 7211 7911 | info@dencrypt.dk | www.dencrypt.dk

ENCRYPTION USED BY NATO & THE DANISH DEFENCE

COMMON CRITERIA CERTIFIED

DENCRYPT

DENCRYPT TALK

Technical Specifications

Voice and Data Encryption

Secure end-to-end-encrypted voice communication and chat using Dynamic Encryption, which ensures that each call session is encrypted with a randomly chosen algorithm and randomly chosen keys.

- Patent pending: PCT/EP2012/071314
- AES-256 + 128-bit seed for dynamic encryption algorithm selection
- Voice: Counter mode (CM) operation
- Live chat: Cyclic Block Chain (CBC) operation PKCS7 padding
- 3K Diffie-Hellman (DH-RSA 3072) for key exchange over the zRTP protocol
- SAS: Four letter readout based on key authentication
- Perfect Forward Secrecy: Encryption key and dynamic algorithm seed established at call setup and removed at call termination
- Key material is generated with cryptographically secure random number generator using the Yarrow algorithm

Local Dencrypt Server System

The Dencrypt Server System, required for Dencrypt Talk, is delivered as an in-house enterprise solution, or it can be provided as a hosted service managed by Dencrypt.

Mutually Authenticated Connections

The Dencrypt Talk app registers in the Dencrypt Server System for activation, call setup and phonebook download, using mutually authenticated connections.

- TLS1.2 Cipher Suite: TLS_EDCH_RSA_WITH_AES_256_GCM_SHA384
- Elliptic curve: secp384r1
- X509 Certificates: RSA 3072 bits. SHA512

Audio

- Constant bit-rate for enhanced security
- Polyphonic ringtones

Platforms

- iOS 10.0 and later
- Android 7.1 or later

Common Criteria and Accreditation

Dencrypt Talk (iOS) is Common Criteria certified (EAL4+) and accredited for classified information up to RESTRICTED. Security target is available on request.

DENCRYPT Arnold Nielsens Boulevard 72 | DK-2650 Hvidovre | Phone: +45 7211 7911 | info@dencrypt.dk | www.dencrypt.dk