ENCRYPTION USED
BY NATO & THE
DANISH DEFENCE

DENCRYPT

DENCRYPT MESSAGE

Encrypted Mobile Communication

Dencrypt Message protects your smartphone instant messaging with state-of-the-art Dynamic Encryption of non-secure digital infrastructure such as WiFi hotspots, mobile networks and satellite links. Dencrypt Message is a user-friendly smartphone application available from App Store and Mobile Device Management systems that support text messaging and content sharing.

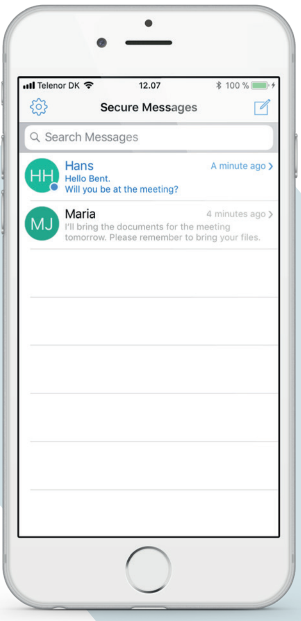
Dynamic Encryption

User-friendly

Text and Attachments

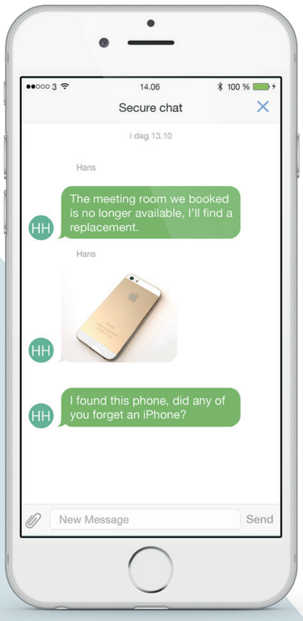
Feature Set

- Dynamic Encryption + AES-256
- End-to-end encryption
- Encrypted text messaging
- Encrypted content sharing:
  - Photos from album or captured by camera
  - Voice clips from file or captured by phone
  - GPS location
- Group messaging
- Secure phone book:
  - Centrally managed
  - Individual call groups
- Secure provisioning
- Connectivity on all cellular and wireless networks
- Mutually authenticated connections
- iOS and Android



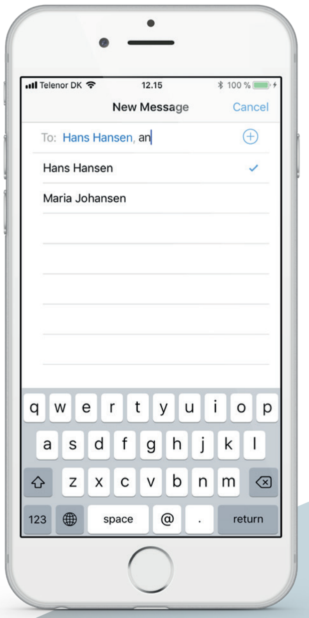
Hans — A minute ago
Hello Bent.
Will you be at the meeting?

Maria — 4 minutes ago
I'll bring the documents for the meeting tomorrow. Please remember to bring your files.



Hans: The meeting room we booked is no longer available, I'll find a replacement.

Hans: I found this phone, did any of you forget an iPhone?



To: Hans Hansen, an

Hans Hansen ✓

Maria Johansen

DENCRYPT MESSAGE

Technical Specifications

Data Encryption

Secure end-to-end encrypted instant messaging and content sharing using Dynamic Encryption, which encrypts each message with a randomly chosen algorithm and randomly chosen keys.

- Patent pending: PCT/EP2012/071314
- AES-256 + 128-bit seed for Dynamic Encryption algorithm selection
- Cyclic Block Chain (CBC) operation. PKCS7 padding
- 3k PKI-based key exchange
- Key material is generated with cryptographically secure random number generation 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.

Connectivity

Instant messaging over cellular, wireless and satellite networks, including 2G/3G/4G/WiFi.

Mutually Authenticated Connections

The Dencrypt Talk app registered to the Dencrypt Server System for provisioning, call set-up and phone book can be downloaded 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

Content Sharing

- Images stored on device or captured directly by the camera
- Sound clips stored on device or captured directly from microphone
- GPS location and map thumbnail

Platforms

- iOS 10,0 and later
- Android 7.1 or later.