ENCRYPTION
USED BY NATO &
THE DANISH DEFENCE

DENCRYPT

DENCRYPT CONNEX

SECURE MOBILE COMMUNICATION

Connex protects your smartphone conversations with state-of-the-art Dynamic Encryption over non-secure digital infrastructure such as WiFi hotspots, mobile networks and satellite links. Connex is a user-friendly smartphone application featuring end-to-end encrypted voice and messages. The app is delivered from app stores or a Mobile Device Management system.

FEATURES

Dynamic Encryption

User-friendly

Enterprise or Cloud solution

Security
» Dynamic Encryption + AES-256
» End-to-end encryption
» Perfect Forward Secrecy
» Trusted connections using TLS1.2
» Secure storage of chat history
» Encrypted push notifications
» Secure provisioning

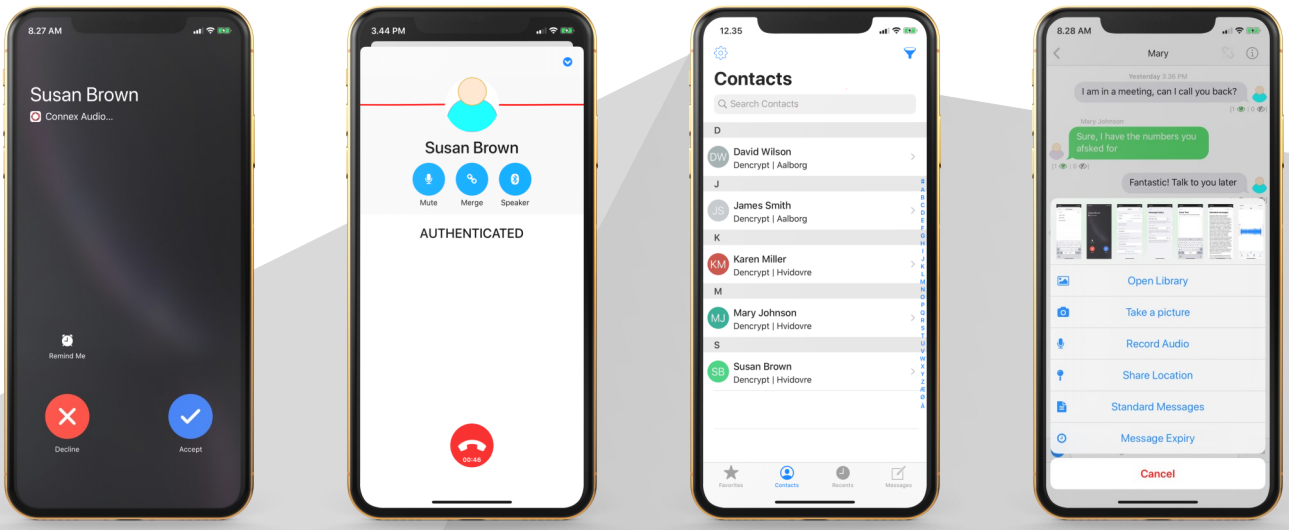
Functionality
» Encrypted voice calls
» Encrypted instant messaging (IM)
  » Text, photos, audio, location
  » Time-constrained IM
» Group calls and messaging
» Excellent audio quality
» Individual, centrally managed contact list

Managed Application
» Dencrypt Control Center (web interface):
  » Call group management
  » Feature configuration
  » Certificate management incl. revocation

Connectivity
» 3G/4G/5G/WiFi

Platforms
» iOS, Android

Certifications
» Common Criteria EAL4+ALC-FLR.2 (ultimo 2020)



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

ENCRYPTION
USED BY NATO &
THE DANISH DEFENCE

DENCRYPT

DENCRYPT CONNEX

Technical Specifications

Voice & Data Encryption

Secure end-to-end encrypted voice and message communication using patented Dynamic Encryption ensuring that each call and message is encrypted with a randomly chosen algorithm and randomly chosen keys.

Voice

» AES-256 + Dynamic Encryption in GCM, 384-bits

» Key exchange over DTLS-SRTP:

» Cipher suite:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

» Elliptic curve: secp384r1

Messages in Transit

» AES-256 + Dynamic Encryption in GCM, 384-bits

» Key exchange over X3DH + Double Ratchet

» Elliptic curve: X448

Messages at Rest

» AES-256 + Dynamic Encryption in GCM, 640-bits

» Dual-keys stored on device and server

» Key exchange over mutually authenticated TLS1.2

Push Notifications

» AES-256 in CFB

» Key exchange over mutually authenticated TLS1.2

Mutually Authenticated Connections

Connex registers in the Dencrypt Server System for provisioning, call setup and phonebook download using mutual authenticated connections.

» TLS1.2 Cipher Suite:

» TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

» Elliptic curve: secp384r1

» Authentication: RSA 3072 bits

Dencrypt Server System

The Dencrypt Server System is available as an Enterprise solution for on-premises installation or as a cloud service managed by Dencrypt.

Connectivity

Voice-over-IP calls and messaging over cellular, wireless and satellite networks, including 3G/4G/5G/WiFi.

Audio

» Constant bit-rate for enhanced security

» Speex and Opus audio codec for excellent audio quality

Platforms

» iOS 12.0 and later

» Android 9.0 or later

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