



BUILDING TRUST

High-End, Secure Mobile Communication
with Military Grade Encryption



SECURE MOBILE COMMUNICATION

In most industries, mobile communication takes place on smartphones that operate on mobile and wireless networks. Many different applications can be used for voice communication, messaging and file transfer, but they all entail risks. Dencrypt is the trusted supplier that helps organisations keep their communication secure.

The consequences of information leaks can be devastating in most industries, so secure mobile communication is paramount. There are many providers of communication products, and also many incidents of data leaks and back doors. Dencrypt is the supplier of secure communication that your organisation can trust.

Dencrypt is based in Denmark and has grown out of a university environment. Our encryption solutions are based on groundbreaking technology that is among the most secure in the world. That means that you can trust Dencrypt's technology to be independent and secure.

Secure mobile communication is particularly important in four sectors – and Dencrypt delivers state-of-the-art solutions to all of them.

GOVERNMENT A matter of national interest

Governments and ministries constantly negotiate and finalise agreements that are critical for national security, trade and the protection of vital infrastructure. Confidential information in the wrong hands can be disastrous, so it is crucial that no information is leaked.

At the same time, information needs to be disseminated fast and effortlessly. It is important that

communication can take place via smartphones, and time is a factor, which makes secure mobile communication essential at government and ministerial levels. Dencrypt provides the encryption solutions that are the answers to this challenge.

BUSINESS Protecting business-critical information

Multinational companies are in constant, global communication, the majority of which is mobile. Information must flow freely inside the company, but at the same time it is highly sensitive to outside listeners. Powers and companies with malign intent may gain an unfair advantage in a competitive world if they gain access to product secrets or information about impending deals and agreements, corporate takeovers, intellectual property etc.

For modern businesses, secure mobile communication is a matter of survival – and Dencrypt has the right solutions to keep business-sensitive information inside your organisation.

MILITARY Military grade encryption

For obvious reasons, military operations and command routes must be kept safe. The military has always had secure communication channels for

landlines and radio-based communication in place. Nowadays, mobile technology is part of military communication practices, and the ability to secure this communication is a matter of life and death. The consequences of leaks of information about imminent operations against terrorists or other enemies of the state would be immense for any nation and its international partners.

Dencrypt supplies secure mobile communication solutions to NATO and the Danish Defence.

POLICING Encryption for law and order

For the police and security companies, it is of utmost importance that information can be passed on quickly. But it is also pivotal that mobile communication is secure. The consequences of someone gaining insight into a police operation – such as terrorist investigations, protection of witnesses, impending actions against criminal groups or transportation of criminals – would be disastrous.

For police forces around the world, flexible and secure communication solutions are essential – and Dencrypt provides these solutions.

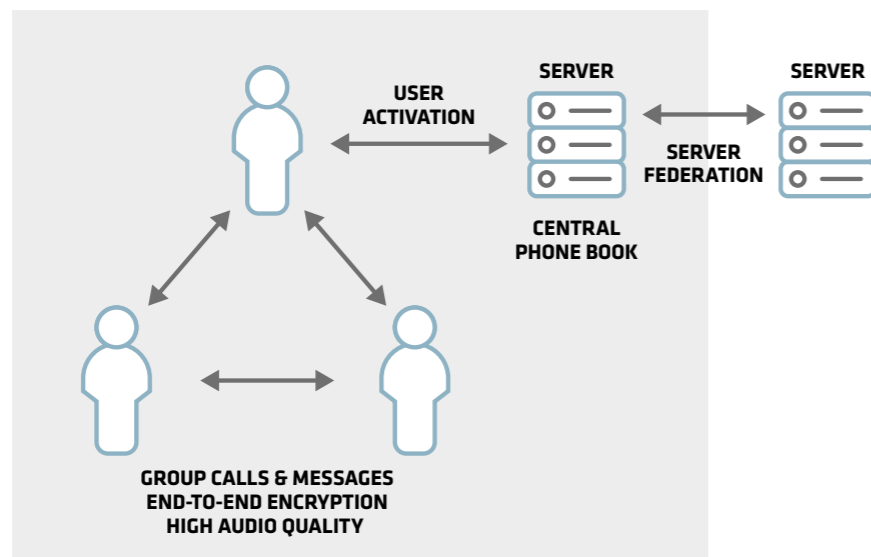


SECURITY IN EVERY DETAIL

Dencrypt's solution is designed with security in mind at every level. Protection of transmitted data is at the heart of our solution that also focuses on secure user management. We have implemented features that protect communication and user data and enable secure administration of users and systems.

The key security features in our solution include:

- » **Dynamic Encryption** – enhances protection of user data
- » **End-to-end encryption** – full protection of data in transit
- » **Secure phonebook**
 - » **Individual contact lists** – enables user-specific phonebooks
 - » **Centrally managed** – means that only authorised users are enrolled
- » **Secure provisioning** – enrolls new users securely
- » **Mutually authenticated connections** – ensure that only trusted clients and servers can communicate
 - » **Server authentication** – prevents clients from connecting to a fake server system
 - » **Client authentication** – prevents fake clients from connecting to the server system and is used to block access from lost or stolen phones
- » **VoIP tunnel** – prevents blocking of VoIP calls in mobile networks
- » **Enterprise deployment** – provides full control of system operation and user data
- » **Root certificate** – enables signing of certificates by customer's root certificate as an ultimate trust anchor



PROTECTED WITH DENCRYPT

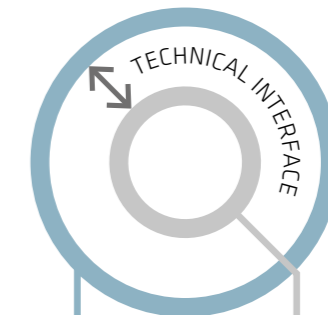
NATO and the Danish Defence have chosen Dencrypt's encrypted communication solution because it ranks among the most secure in the world. Our solution was developed in a high-integrity, independent environment.

Dencrypt's Dynamic Encryption is a unique encryption algorithm that gives you the ultimate protection. The core encryption – for example a standard AES 256 algorithm – is wrapped by an additional dynamic encryption layer where encryption keys and the encryption algorithm are changed for each new data transmission. This ever-changing cryptosystem provides a moving target defence and makes automated attacks by an adversary impossible.

Dynamic Encryption was invented by Lars Ramkilde Knudsen, a renowned professor of cryptology at the Technical University of Denmark. The invention is referred to by peers as state-of-the-art cryptology.

Our solution was developed in Denmark, a country known for the world's lowest corruption level, high integrity and complete independency of private companies from government and authorities. For our customers, this means that not only are our algorithms and technology of the highest standard, but you can also trust that our solution has no hidden back doors or potential circumventions of the encryption. This guarantee is backed by our Common Criteria certification and NATO RESTRICTED accreditation.

MULTI-LAYER PROTECTION WITH DYNAMIC ENCRYPTION



- » Dynamic Encryption layer
- » New key and random encryption algorithm for each call
- » Inner algorithm – AES 256 or any other crypto algorithm
- » New key for each call

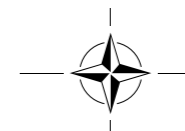
FEATURES

- » End-to-end encryption
- » High audio quality
- » Group calls and messages
- » Secure phone book and user activation
- » Connectivity on all cellular and wireless networks
- » Available as cloud service or enterprise solution
- » Runs on standard iOS and Android smartphones

ENCRYPTION USED BY THE DANISH DEFENCE



ENCRYPTION USED BY NATO




COMMON CRITERIA CERTIFIED





DENCRYPT CONNEX

Secure Mobile Communication App

Connex is a user-friendly smartphone application that protects your smartphone conversations with state-of-the-art Dynamic Encryption over non-secure digital infrastructure such as Wi-Fi hotspots, mobile networks and satellite links. It features end-to-end encrypted voice, video, and messages. The app is delivered from app stores or a mobile device management system.

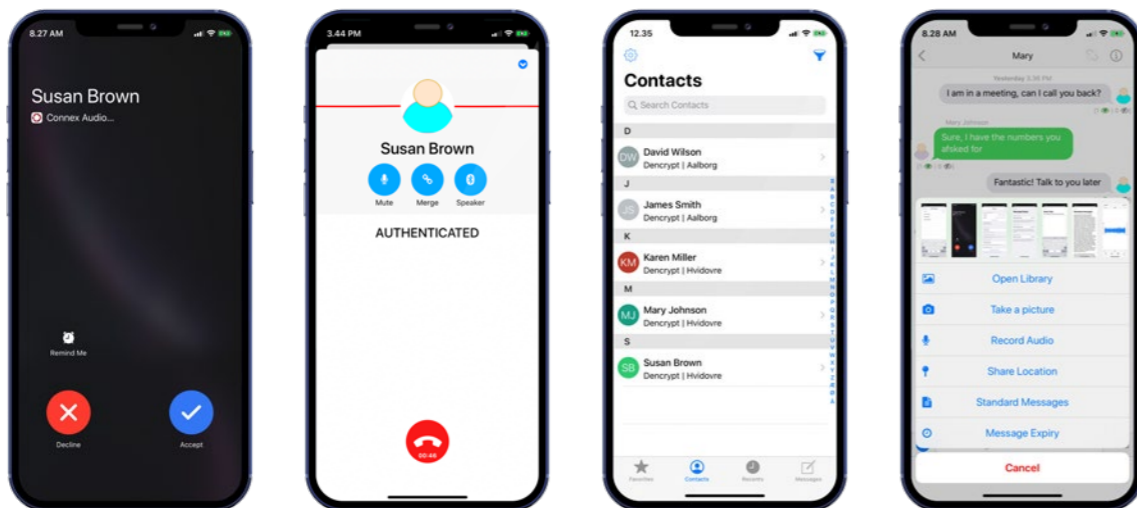
- 

Dynamic Encryption
- 

User-friendly
- 

Certified and accredited

FUNCTIONALITY	SECURITY	MANAGED APPLICATION
<ul style="list-style-type: none"> » Encrypted voice and video calls » Encrypted instant messaging (IM) <ul style="list-style-type: none"> » Text, photos, audio, location » Time-constrained IM » Group calls and messaging » Excellent audio quality » Individual, centrally managed contact list » 3G/4G/5G/Wi-Fi » iOS, Android » Common Criteria EAL4+ALC-FLR.2 	<ul style="list-style-type: none"> » 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 	<p>Dencrypt Control Center (web interface):</p> <ul style="list-style-type: none"> » Call group management » Feature configuration » Certificate management including revocation



DENCRYPT SERVER SYSTEM

Secure Communication Platform

The Dencrypt Server System provides infrastructure that enables secure mobile communication using the Dencrypt smartphone applications. Dencrypt Server System is Common Criteria certified. It is delivered as a cloud service or as an enterprise solution for organisations that require full control of all parts of their communication solution.

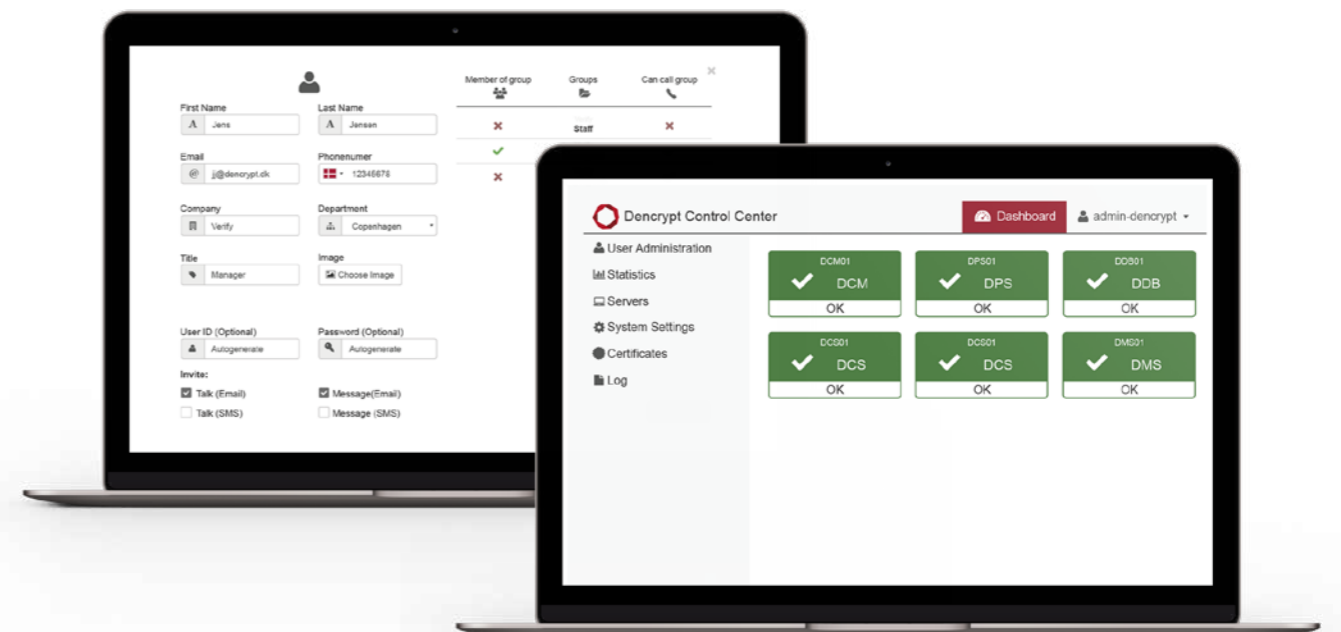
- 

Enterprise or cloud solution
- 

Web-based user interface
- 

Certified and accredited

SECURITY	DENCRYPT CONTROL CENTER
<ul style="list-style-type: none"> » Secure call set-up » Secure message routing » Secure activation of end-users » Audit and event logs » Trusted connections using TLS1.2 » Mutual authentication » Common Criteria certified (ISO 15408) at EAL2+ 	<p>Web-based management tool</p> <ul style="list-style-type: none"> » Role-based administration » User management » Call group and phone book management » User revocation » Certificate management » Call statistics » System status dashboard





DENCRIPT

Arnold Nielsens Boulevard 72

DK-2650 Hvidovre

Denmark

Phone: +45 7211 7911

info@dencrypt.dk

www.dencrypt.dk