ENCRYPTION USED BY NATO & THE DANISH DEFENCE

COMMON CRITERIA CERTIFIED

DENCRYPT

DENCRYPT SERVER SYSTEM

Encrypted Mobile Communication

The Dencrypt Server System provides infrastructure that enables secure mobile communication using the Dencrypt Talk and Dencrypt Message smartphone applications. Dencrypt Server System is Common Criteria certified and is delivered as an enterprise solution for organisations requiring full control of all parts of their communication solution.

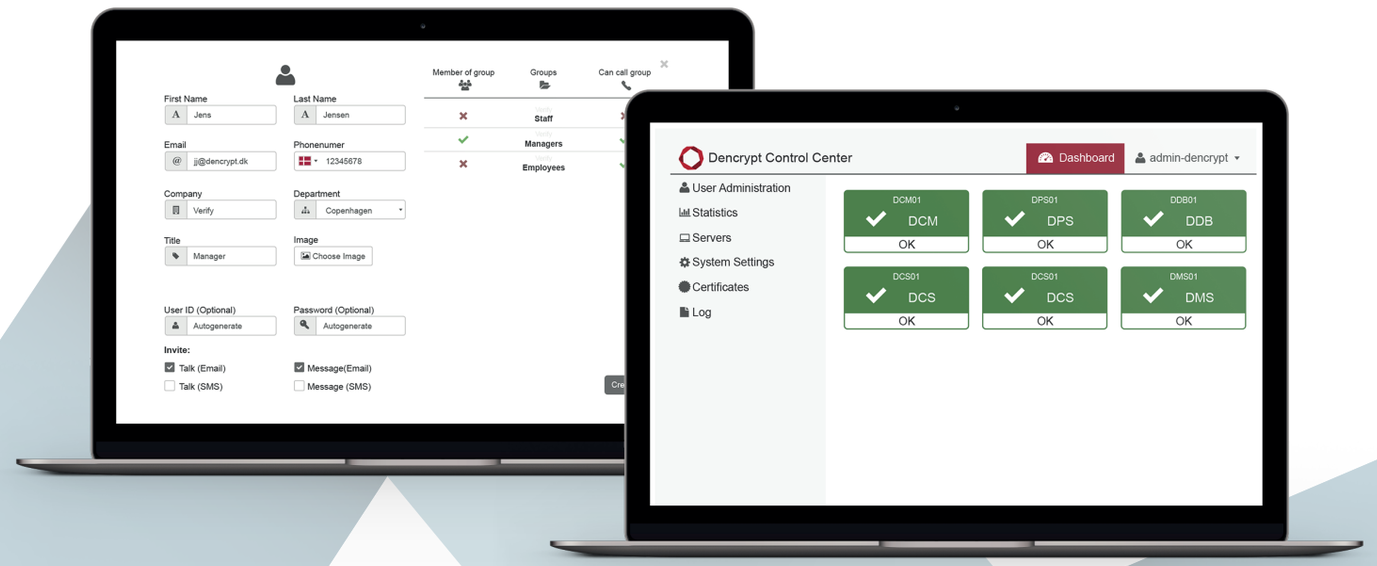
In-house Deployment

User-friendly

Certified and Accredited

Feature Set

- Secure voice 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+
- Dencrypt Control Center – web-based management tool:
  - Role-based administration
  - User management
  - Call group and phonebook management
  - User revocation
  - Certificate management
  - Call statistics
  - System status dashboard



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 SERVER SYSTEM

Technical Specifications

Enterprise Solution

The Dencrypt Server System is deployed on virtual machines and managed within the organisation's IT environment for full control of operations and user management.

Deployed by Dencrypt personnel and delivered as a turn-key solution ready for use, the Dencrypt Server System is also offered as a hosted service by Dencrypt for fast rollout and a minimum of overhead costs.

End-to-end Encryption

The Dencrypt Server System only facilitates the secure voice call set-up and message routing. It does not decrypt voice calls or message content.

Dencrypt Control Center

The Dencrypt Control Center is an easy-to-use web-based management tool for user administration, system monitoring and call statistics. It can be operated without special skills and with a minimum of training.

Common Criteria and Accreditation

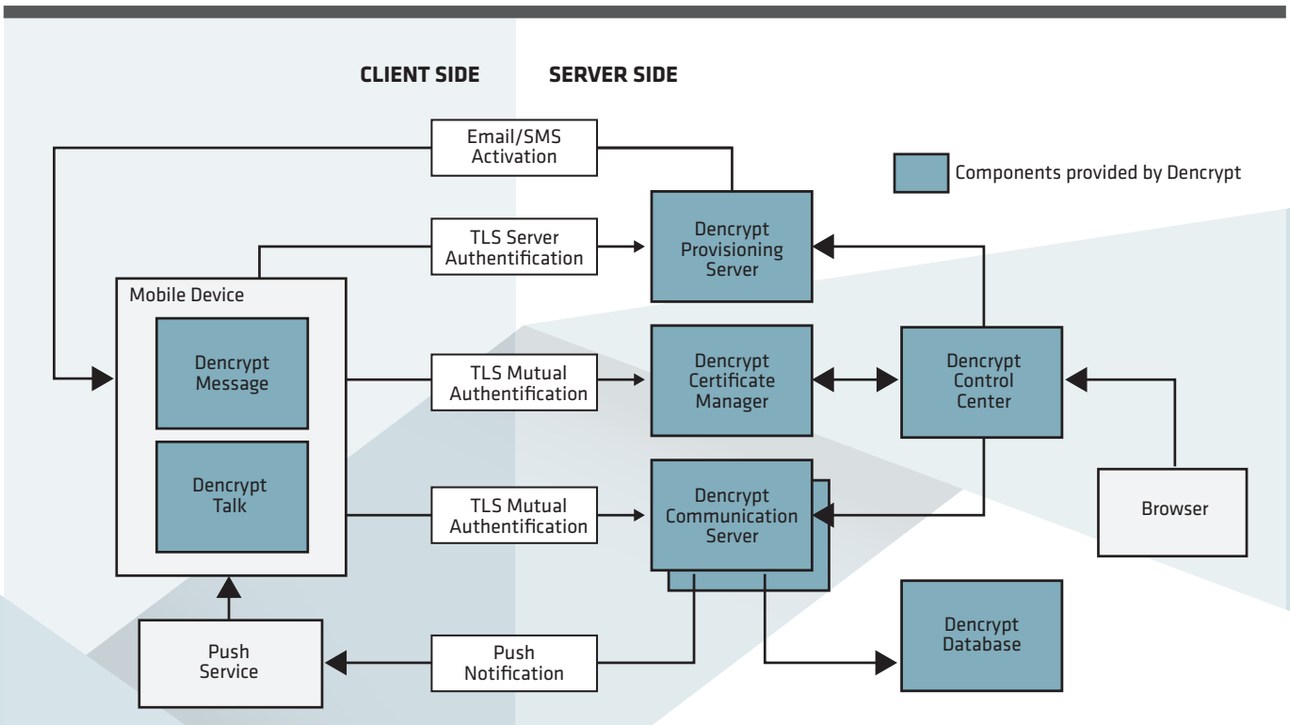
The Dencrypt Server System is Common Criteria-certified (EAL2+) and accredited for classified information up to RESTRICTED. Security target is available on request.

Connections:
» TLS1.2: TLS_EDCHE_RSA_WITH_AES_256_GCM_SHA384
» Elliptic curves: secp384r1

RSA key generation and signing:
» RSA4096 bits
» RSA3072 bits (temporary key for activation)

X509 certificates:
» RSA4096 bits
» SHA512

Random number generation:
» OpenSSL RNG from Debian Linux
» SHA512



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