DENCRYPT

Dencrypt Communication Solution

# Preparative guide & hosting requirement

## Dencrypt Server System 5.0

Version 1.2


19-08-2020

Company Restricted

# Contents

# 1 Introduction

## 1.1 Product versions

This guide applies for Dencrypt Server System v. 5.0 consisting of the following components Figure 1:

- Dencrypt Certificate Manager (DCM)
- Dencrypt Provisioning Server (DPS)
- Dencrypt Control Center (DCC)
- Dencrypt Database (DDB)
- Dencrypt Communication Server (DCS)
- Dencrypt System Bridge (DSB)

## 1.2 Content

This guide is intended for IT-professionals responsible for preparing an IT-environment to host a Dencrypt Server System. The guide provides detailed requirements to the IT-environment and also serves as a checklist before starting the installation procedure.

The document has the following content:

- Installation procedure
- Requirements to the IT-environment
- Checklist

## 1.3 System architecture

The Dencrypt Communication Solution is depicted in Figure 1 and consists of a client application installed to end-users mobile devices and the Dencrypt Server System deployed within a secure IT-environment. The Dencrypt Communication Solution consists of the following components:

- **Dencrypt Connex**
  Dencrypt Connexis the mobile client, which provides secure voice and instant messages using the SIP protocol. The client must be provisioned before taken into use. This is done using the Dencrypt Provisioning server.
- **Dencrypt Provisioning Server (DPS)**
  The Dencrypt Provisioning Server (DPS) is used to initialize clients with login credentials and client certificates to communicate with the system's server. The client is provided with an HTTPS web-link for the initialization. The link shall be delivered to the end-user in a secure way and not disclosed during transmission. The DPS provides the means for secure transmission.
- **Dencrypt Communication Server (DCS)**
  The Dencrypt Communication Server (DCS) provides the SIP services necessary for the Clients to establish secure voice calls between two or more clients and for the message exchange between clients. The system allows for multiple instances of DCSs for logical redundancy and load balancing. The DCS is also responsible for generating and distributing phonebooks and settings to the clients. The DCS includes a LiME server, which facilitates the key exchange for secure messaging.

- **Dencrypt Database (DDB)**
  The Dencrypt Database (DDB) provides database services for the system. It stores data and logs for end-users, statistics, servers and connections. Furthermore, it stores the secure messages waiting for delivery and facilitates the key exchange protocol.
- **Dencrypt Control Center (DCC)**
  The user management and server administration is performed using the Dencrypt Control Center (DCC). This includes creating/deleting users and manage contact groups. The DCC offers a web interface accessible from a web browser from the administrator's local machine.
- **Dencrypt Certificate Manager (DCM)**
  The Dencrypt Certificate Manager (DCM) is the central point for TLS certificates in the system. Once provisioning has taken place, all connections between Dencrypt Connexand Dencrypt Server System use mutually authenticated TLS connections. The required TLS certificates are issued by the Dencrypt Certificate Manager. The DCM also issues TLS certificates for internal server validation.
- **Dencrypt System Bridge (DSB)**
  The Dencrypt System Bridge (DSB) handles all communication between external Dencrypt systems. It is used as a gateway to federated systems including certificates for mutual authentication towards external Dencrypt Server Systems.

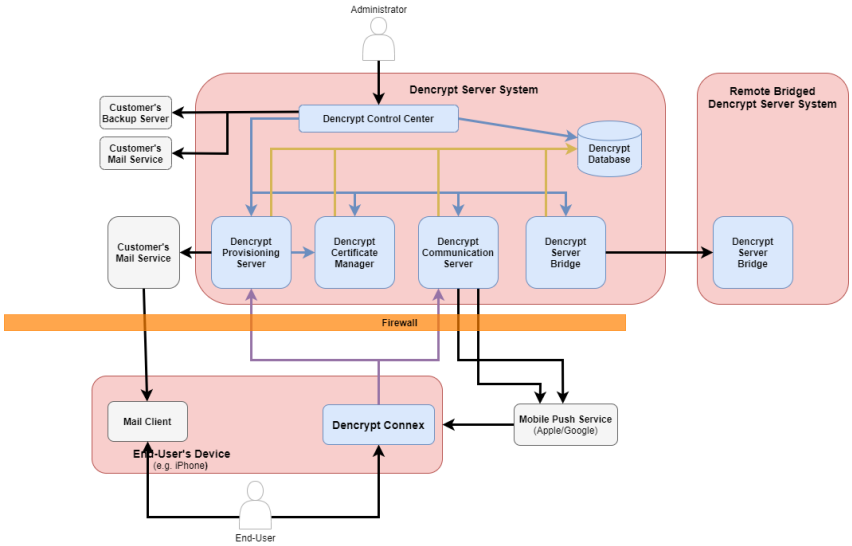


Figure 1: Dencrypt Communication Solution overview

## 1.4 Authenticated connections

All connections between Dencrypt Connexand the Dencrypt Server System (DSS) are mutual authenticated TLS connections. The Dencrypt Certificate Manager (DCM) issues intermediate certificates signed by the Dencrypt root CA and distributed via the Dencrypt Provisioning Server (DPS) or Dencrypt Communication Server (DCS).

### 1.4.1 Server validation

Server certificates issued for the external TLS connections are also used for internal connections between server components. The Dencrypt Control Center is authenticated by the administrator's browser.

### 1.4.2 App validation

A signed certificate on the Dencrypt Connexclient is established by the client sending certificate signing request to the Dencrypt Provisioning Server (DPS), which returns the client certificate in the response.

# 2 Security instructions

The Dencrypt Server System shall be hosted in a secure environment, which shall ensure:

- That the Dencrypt Server System is protected against physical access.
- That the Dencrypt Server System is protected against untrusted networks by a well-configured firewall (section 4.5.2)
- That the hardware and local network is dedicated and configured to support both functional and security-related requirements.
- That only authorized and trained IT-professionals have access to the system.
- That the system is operated and managed by IT-professional trusted by the organization, non-hostile and capable of following their guidance.
- That the end-users of Dencrypt Connexare trustworthy, non-hostile and have received training to perform their actions in accordance with their instructions and security policies.

# 3 System installation

Dencrypt personnel or a technical partner is responsible for the physical installation and configuration of the Dencrypt Server System with the active participation of IT-professionals from the Customer organization. After a successful deployment, the system is handed-over to the Customer for operational use.

The procedure for a system installation is:

1. **Kick-off meeting** with the Customer's IT-professionals to:
   (a) provide an introduction to the Dencrypt Communication Solution and its components.
   (b) to explain the functional and security related requirements to the IT environment listed in this document
   (c) agree on a plan for the preparations of the IT-environment, the physical installation and handover.
   (d) provide the Customer with a copy of the test case list for the acceptance test [2].
2. **Preparation of the IT-environment.** The Customer's system administrator shall prepare the IT environment according to the requirements listed in this document.
   The customer will report the IT-environment "Ready for installation" when the requirements listed in section 4 have been met. Firewall settings for system installation shall be applied as described in table 5)
   The checklist in section 5 shall be completed and the configuration details in section 4 shall be filled and returned to Dencrypt.
3. **SW installation.** Dencrypt (or a technical partner) will verify that the checklist (section 5) has been completed and all required configuration details have been provided, before performing the SW installation.
   Two options exist for the deployment and physical installation depending on the availability of a VPN connection to the IT-environment:
   (a) Physical installation at the customer's premises in case a VPN connection cannot be provided. Dencrypt will bring the SW as .iso images on a USB media.
   (b) Remote installation via a customer provided VPN connection to the Virtual Machine (VM) management. Dencrypt will upload and install the .iso images over the VPN connection.
   Dencrypt will perform an internal test and verification of the entire system. The Customer shall apply firewall settings for normal operation (table 5)
   Dencrypt will report the system "Ready for Acceptance".
4. **Acceptance test and handover.** Together with the Customer, Dencrypt will perform an acceptance test, training of system administrators and handover the system to the Customer for operational use.
   The acceptance test will be performed together with the responsible person from the Customer organisation, who shall sign the acceptance test case list when all applicable tests have passed.
   The system training shall at least include the appointed system administrator (section 4.15) and will contain:
   (a) a walk-through of the operational user guide for Dencrypt Connex[3], while demonstrating functionality and procedures on the Dencrypt Connexapplication.
   (b) a walk-through of the operational user guide for Dencrypt Server System [4], while demonstrating the functionality and procedures on the Dencrypt Control Center.
   (c) Instructions for reporting errors and security incidents [1].
   After the system training the system administrator shall be able to train and provide security instructions to Dencrypt Connexend-users and administrators of the Dencrypt Server System. The acceptance test and system training can take place simultaneously.
   At handover Dencrypt will provide a URL and login credentials to the Dencrypt Control Center for the following administrator roles [4]:

(a) *System Admin* to be used for the daily system operation.

(b) *Service Access.* System access reserved for Dencrypt (or partners) for service and maintenance updates. The System Admin is required to store the credentials securely and ensure that they are not disclosed. The credentials shall be shared with Dencrypt support prior to a service update.

The Service Access role shall only be used by trained Dencrypt (or partner) personnel.

The system is considered handed over for operational use, when the acceptance test and training has been successfully completed.

# 4 Requirements to the IT-environment

This section list the requirements to the customer's IT-environment to ensure the functionality and security of the Dencrypt Server System. The Customer is responsible to ensure the IT-environment fulfills the minimum requirements.

Each section serves as a checklist for the Customer to fill, to ensure that all requirements to the IT-environment have been met and that the required information has been provided to Dencrypt.

## 4.1 Minimum requirements

Each server component is deployed using `.iso` images on a dedicated server, which can be either physical or virtual. The minimum requirements for each server component is listed in table 1.

| Component | DCS01 | DCS02 | DPS | DCM | DCC | DDB |
|---|---|---|---|---|---|---|
| **CPU** | 2 x 3 GHz | 2 x 3 GHz | 1 x 2 GHz | 1 x 2 GHz | 1 x 2 GHz | 1 x 2 GHz |
| **RAM** | 4 GB | 4 GB | 1 GB | 1 GB | 1 GB | 4 GB |
| **HDD** | 100 GB | 20 GB | 20 GB | 20 GB | 100 GB | 60 GB |
| **Network** | 1GB/s | 1GB/s | 1GB/s | 1GB/s | 1GB/s | 1GB/s |

Table 1: Minimum requirements including back-up.

Notes:

- The backup service requires additional disk space for DCS01, DDB and DCC for prepare the backup bundle for uploaded to the back-up destination.
- These are estimated minimum requirements, which may be adjusted according to the usage.

## 4.2 Server firmware

Each server shall be updated to the latest firmware and the latest security patches shall be applied.

## 4.3 Domain and network adresses

### 4.3.1 Public IP Addresses via NAT

A single local IP-address is assigned to each server and located behind a NAT. At the outside of the NAT three (3) public IP-adresses are defined in the DNS configuration:

- A public IP-address for DCS01.
- A public IP-address for DCS02.
- A public IP-address shared by the DPS and DCM.

The traffic flow is illustrated in figure 2 and the port mappings are defined in table 2. The public IP-addresses for DCS01 and DCS02 are part of the internal configuration and changes to the DNS records require a reconfiguration of the server system.

The Customer shall provide a firewall between the internet and the server system as specified in section 4.5.2

An internal firewall setup between server components as specified in section 4.5.3 is recommended.

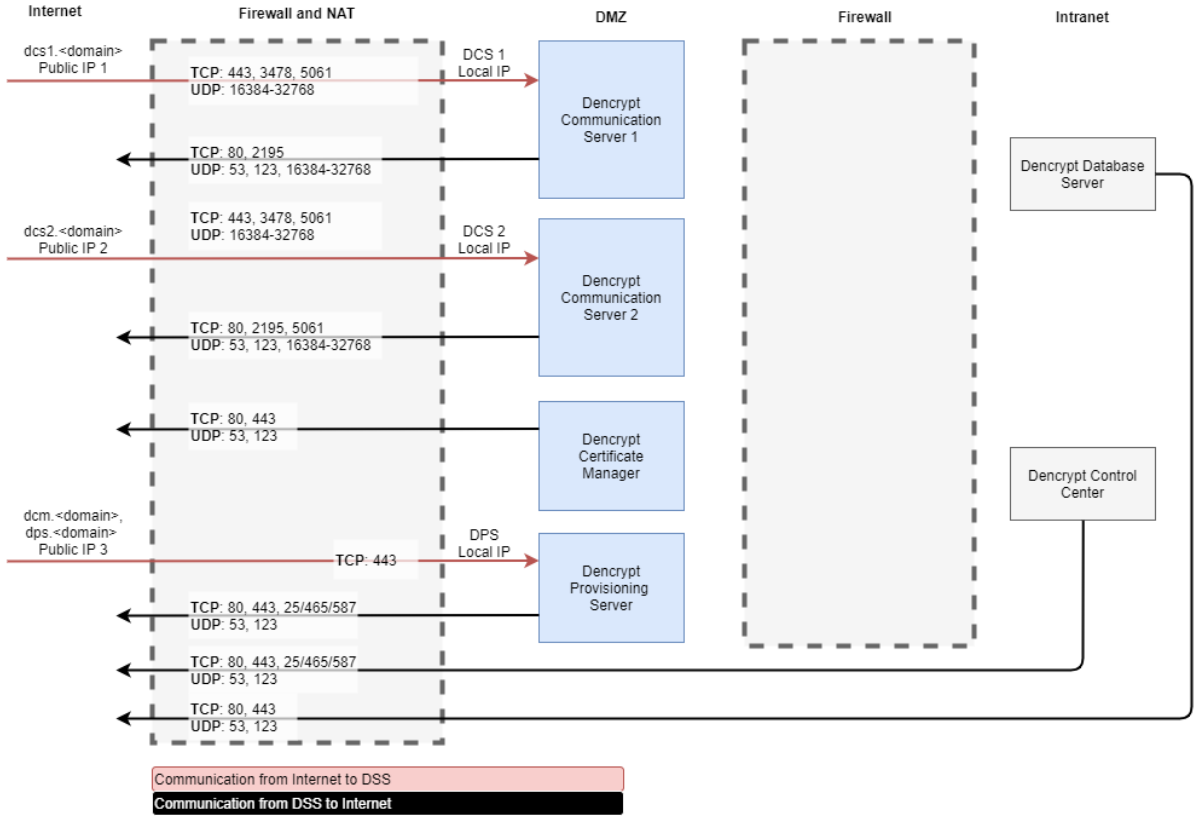


Figure 2: Firewall and NAT between internet and DMZ

| Server | Internet | DMZ | NAT type | NAT outer port | NAT inner port |
|---|---|---|---|---|---|
| **DCS01** | Public IP 1 | Local IP 1 | 1-to-1 | All (TCP+UDP) | All (TCP+UDP) |
| **DCS02** | Public IP 2 | Local IP 2 | 1-to-1 | All (TCP+UDP) | All (TCP+UDP) |
| **DPS01** | Public IP 3 | Local IP 3 | 1-to-many | 443 | 443 |

Table 2: NAT port mapping

### 4.3.2 Template for domain and network adresses

The Customer is required to provide network domains and addresses for the local installation by completing table 3. Dencrypt will use the information provide to configure the Dencrypt Server System.

| Component | Domain | Global IPv4 | Local IPv4 | Netmask | Gateway | Name server |
|---|---|---|---|---|---|---|
| **System** | *system.example.com* | NA | NA | NA | NA | NA |
| **DCS01** | *dcs01.system.example.com* | | | | | |
| **DCS02** | *dcs02.system.example.com* | | | | | |
| **DPS** | *dps01.system.example.com*<br>*activate.system.example.com* | | | | | |
| **DCC** | NA | NA | | | | |
| **DDB** | NA | NA | | | | |

Table 3: Domain and network addresses.

There must be two DNS records for the DPS, i.e:

- Ex. *dps.system.example.com* (A record)
- Ex. *activate.system.example.com* (A or CNAME record)

Substitute *example.com* with the actual system domain name.

## 4.4 Service Records (SRV)

The VoIP and STUN services of the Dencrypt Communication Solution deploy service records (SRV). The domain name entry for the VoIP and STUN services specified the DCS01 and DCS02 addresses. Table 4 shows an example of the SRV record entries, assuming these example addresses for DCS01 and DCS02:

- DCS01 domain: *dcs01.system.example.com*
- DCS02 domain: *dcs02.system.example.com*

| # | Domain | Type | TTL | Pri. | Weigth | Port | Location |
|---|---|---|---|---|---|---|---|
| **1** | _sips._tcp.dcs.system.example.com | SRV | 86400 | 10 | 100 | 5061 | dcs01.system.example.com |
| **2** | _sips._tcp.dcs.system.example.com | SRV | 86400 | 20 | 0 | 5061 | dcs02.system.example.com |
| **3** | _stun._udp.dcs.system.example.com | SRV | 86400 | 10 | 100 | 3478 | dcs01.system.example.com |
| **4** | _stun._udp.dcs.system.example.com | SRV | 86400 | 20 | 0 | 3478 | dcs02.system.example.com |

Table 4: Example of SRV record with logical failover.

## 4.5 Firewall and external network ports

### 4.5.1 Secure start-up

Prior to starting the installation procedure, the firewall shall block all ingoing external communication to the Dencrypt Server System. Only, the following traffic shall be allowed during the installation process:

- VPN connection, if available.
- Outgoing traffic

Once the system installation has completed successfully, the firewall settings for normal operation shall be applied to perform validation and acceptance test. The Customer shall provide access to a technical-skilled person with the authority to perform firewall configuration.

### 4.5.2 Firewall configuration of external ports

Table 5 lists the required configuration for the firewall and external ports. The mapping of external ports to internal ports has to be implemented for each server.

To ensure the security of the system all other ports shall be blocked.

| Port | Source | Destination | Traffic | Service |
|---|---|---|---|---|
| **22** | DCC | Backup server | TCP | SCP destination for dencrypt backup. |
| **25** | DPS | SMTP mail server | TCP | Send emails for invitations and notifications. |
| **53** | DCS01, DCS02 DCM, DPS, DDB, DCC | DNS server | TCP<br>UDP | DNS lookup. |
| **80** | DCS01, DCS02 DCM, DPS, DDB, DCC | mirrors.dencrypt.dk | TCP | Package download. |
| **123** | DCS01, DCS02 DCM, DPS, DDB, DCC | NTP server | UDP | Network time protocol. |
| **443** | DCS01, DCS02 DCM, DPS, DDB, DCC | mirrors.dencrypt.dk<br>Google push service<br>Apple push service<br>SMS gateway | TCP | Package download<br>Push notification services<br>SMS gateway service |
| **443** | Any client IP address | DCS01, DCS02, DPS | TCP | HTTPS wep api<br>Provisioning<br>Phonebook/settings download |
| **465** | DPS | SMTP mail server | TCP | Send emails for activation and notifications. |
| **587** | DPS | SMTP mail server | TCP | Send emails for activation and notifications. |
| **2195** | DCS01, DCS02 | Apple push server | TCP | Apple push notification service |
| **3478** | Any client IP address | DCS01, DCS02 | UDP | STUN |
| **5061** | Any client IP address | DCS01, DCS02 | TCP | SIP-TLS |
| **16384-32768** | Any client IP address | DCS0x | UDP | VoIP |

Table 5: Network port configuration

To minimize the failover time in case of Ethernet disconnection or power-off for a DCS server, it is recommended to have an active network component, which sends *icmp-host-unreachable* response.

### 4.5.3 Firewall configuration for internal network

Table 6 lists the recommended firewall configuration for the Dencrypt Server System internal network. The port configuration and data flow for each server component is illustrated in appendix A.

| Port | Source | Destination | Traffic | Service |
|---|---|---|---|---|
| **3000** | DCC | DCS01, DCS02 | TCP | WebAPI |
| **3001** | DCC, DPS | DCM | TCP | WebAPI |
| **3002** | DCS01, DCS02, DCC, DCM, DPS | DCM | TCP | WebAPI |
| **3003** | DCC | DPS | TCP | WebAPI |
| **3004** | DCC | DCS01, DCS02 | TCP | WebAPI |
| **3006** | DCS01, DCS02 | DDB | TCP | MySQL |
| **5059** | DCS01, DCS02 | DCS01, DCS02 | TCP | VoiP clustering |
| **5672** | DCS01, DCS02, DCC, DCM, DPS | DDB | TCP | RabbitMQ |
| **6379** | DCS01, DCS02, DDB | DCS01, DCS02 | TCP | Registration sync. |
| **9000** | DCS01, DCS02 | DDB | TCP | Minio S3 |
| **26379** | DCS01, DCS02, DDB | DCS01, DCS02 | TCP | Registration sync. |

Table 6: Internal network port configuration

## 4.6 Root certificate

The intermediate certificates must be signed by a root certificate authority, which can be the Customer's root certificate authority or Dencrypts root certificate authority.

In the case of signing with a Customer root certificate, Dencrypt will provide a Certificate Signing Request (CSR), which shall be signed by the Customer during the installation process. The Customer must ensure the following X.509 v3 certificate extensions to the intermediate certificate as part of the signing process:

| **Basic constraints:** | |
|---|---|
| Critical | Yes |
| is CA | Yes |
| Path length constraints: | 0 |
| **Key usage:** | |
| Critical | Yes |
| Digital signature | |
| Certificate sign | |
| CRL sign | |

Table 7: X.509 v3 certificate extensions

In case of signing by Customer root authority, the Customer must also produce a Certificate Revoke List (CRL).

Before installation, Dencrypt offer to validate the root certificate and certificate revocation list. The Customer shall provide the public certificate and certification revocation list.

Please indicate the preferred option for root certificate signing in Table 8.

| | |
|---|---|
| **Customer Root CA** | Yes/No |
| **Dencrypt Root CA** | Yes/No |

Table 8: Root certificate signing.

## 4.7 Provisioning link - certificate signing

The activation link for provisioning must have a valid https certificate signed by a public Certificate Authority (CA), to ensure the browser on the device does not reject the activation link.A certificate signing request (CSR) is generated during the system installation and handed over to the Customer. The Customer shall request their CA to sign the request. The CA-signed certificate is installed on the Dencrypt Provision Server (DPS), to enable provisioning of end-users.

It is recommended to request their CA to do a DNS based Domain Control Validation (DCV) as the Dencrypt Server System does not support HTTP/HTTPS based Domain Control Validation.

## 4.8 Communication services for provisioning

End-users must go through a first-time registration process (provisioning) before the app is activated and ready for use. From the DCC the system administrator provides the end-user with a time-limited, one-time activation link in the form of an URL or QR-code. The activation link is delivered to the end-user by secure email, or a printed QR-code. The activation link shall be delivered to the intended user without being disclosed to 3rd parties. When using email, the connections between the email server and email client shall be encrypted.

The provisioning service requires access to the Customers SMTP mail server. The customer is requested to provide the following information for Dencrypt to configure the provisioning services.

| **SMTP mail server for provisioning** | |
|---|---|
| **Mail server address** | |
| **Mail server port** | |
| **Protocol** | SMTP, SSL/TLS |
| **Username** | |
| **Password** | |

Table 9: Configuration of email services for provisioning.

| SMTP mail server for notifications | |
|---|---|
| **Mail server address** | |
| **Mail server port** | |
| **Protocol** | SMTP, SSL/TLS |
| **Username** | |
| **Password** | |

Table 10: Configuration of email services for notifications.

## 4.9 Network time protocal

The IT-environment shall provide a reliable time source for the Dencrypt Server System and for the IT-environment itself. The Dencrypt Server System requires firewall access on port 123 to access a Network Time Protocol (NTP) server (table 5).

## 4.10 VPN remote access (Optional)

### 4.10.1 System installation and maintenance.

Dencrypt offers to perform the system installation as well as service and maintenance using remote VPN access. For system installation, VPN access to the virtual machine (VM) management is required. For service and maintenance, only VPN access to the DSS network is required. The VPN-access is only temporary during system installation and service windows. The VPN software client shall support multi-factor authentication (MFA).

| Port | Traffic | Direction | Peer | Service |
|---|---|---|---|---|
| **22** | TCP | in | DCS01, DCS02, DCM, DPS, DCC, DDB | SSH access for system installation. |
| **443** | TCP | in | DCC | Web-access to Dencrypt Control Center for service. |

Table 11: VPN configuration for system installation and service.

The customer is requested to indicate, whether VPN access is available and provide configuration and access details.

| | |
|---|---|
| **VPN remote access** | Yes/No |
| **Configuration provided?** | Yes/No |

Table 12: VPN remote access.

### 4.10.2 User management

User- and system management is performed by the Customer and require web-access to the Dencrypt Control Center, by:

- a local workstation with network access limited to the Dencrypt Control Center.
- a VPN connection to the Dencrypt Control Center. The VPN client shall use multi-factor authentication (MFA).

| Port | Traffic | Direction | Peer | Service |
|---|---|---|---|---|
| **443** | TCP | in | DCC | Web-access to Dencrypt Control Center for service. |

Table 13: VPN configuration for user and system management.

## 4.11 Corporate Wifi configuration

For the applications to be functional on wifi-networks, the wifi shall be configured as shown in table 14. It is recommended to apply either 802.11k, 802.11r and 802.11v wifi-standards to enable wifi-roaming between access points.

| Port | Traffic | Direction | Peer | Service |
|---|---|---|---|---|
| **443** | TCP | out | DCS, DPS | Web-API for phonebook/settings download |
| **3478** | TCP/UDP | out | STUN server | IP-address resolving service. |
| **5061** | TCP | out | DCS01, DCS02 | SIP-TLS |
| **16384-32768** | UDP | out | Any IP-address | RTP, SRTP, ZRTP |

Table 14: Wifi configuration

## 4.12 Remote backup (optional)

Each server compiles an encrypted archive file containing the data (i.e. configurations, user meta data) required to restore operations after a failure. The encrypted archive files are send to the Dencrypt Control Center for upload via Secure Copy (scp/ssh)to a remote backup destination or for download from the browser interface. Periodic backups can be scheduled from the Dencrypt Control Center.

The requirements to configure a remote backup destination are:

- a backup server supporting *Secure Copy*
- dedicated login credentials to the backup server
- secure storage of the private PGP-key to decrypt the backup.

| Backup service configuration | |
|---|---|
| **Backup server address** | |
| **Backup server port** | |
| **Username** | |
| **Password** | |
| **Remote folder path** | |
| **Backup bundle name** | |

Table 15: Configuration of remote backup

## 4.13 Technical contacts

Provide contact information for the technical persons responsible for the listed areas.

| Remote VPN access | Firewall and network | Virtual machines |
|---|---|---|
| Name: | Name: | Name: |
| Email: | Email: | Email: |
| Phone: | Phone: | Phone: |

Table 16: Technical contacts.

## 4.14 Responsible for acceptance and handover

Provide contact information for the responsible persons for acceptance-test and handover. The person assigned shall be authorized to accept the system on behalf of the organisation.

| Contact for accceptance and handover |
|---|
| Name: |
| Email: |
| Phone: |

Table 17: Contact for acceptance and handover.

## 4.15 System administrator

Please provide the contact information for the System Administrator of the Dencrypt Server System. The assigned system administrator shall:

- be trusted by the organization, non-hostile and capable of following their guidance and have received training to perform their actions in accordance with their instructions and security policies.
- be authorized by the organisation to operate the system with the managerial role which they have been assigned (See [4].
- be a trained IT-professional, which has received training in the secure operation of the Dencrypt Communication Solution.

The system administrator will be granted the *System Admin* role of the Dencrypt Server System and shall be authorized to assign other administrators to the system. The System administrator shall take active participation in the acceptance test and handover of the system.

| **Contact for System Administrator** |
| --- |
| Name: |
| Email: |
| Phone: |

Table 18: Contact for system administrator.

# 5 Checklist

Use the checklist in table 19 to verify that the configuration of the IT-environment complete and return a copy to Dencrypt.

| | Item | Reference | OK | NOK | NA | Notes |
|---|---|---|---|---|---|---|
| **1** | Server instances are ready and fulfill minimum requirements for ISO image deployment by Dencrypt? | Table 1 | | | | |
| **2** | Domains and network parameters are identified?<br>Domains are available and external IP addresses are assigned to domains? | Table 3 | | | | |
| **3** | NAT configuration is performed? | Section 4.3.1 | | | | |
| **4** | Configuration of firewall and ports is performed? | Table 5 | | | | |
| **5** | Root certificate signing | Table 8 | | | | |
| **6** | Agreement with public CA for signing provision server certificate | Section 4.7 | | | | |
| **7** | SMTP mail server configuration shared? | Table 9 & 10 | | | | |
| **8** | Reliable time source established? | Section 4.9 | | | | |
| **9** | Is remote VPN access available?<br>If yes, has configuration and access details been shared? | Section 4.11 | | | | |
| **10** | Configuration of corporate Wifi? | Table 14 | | | | |
| **11** | Technical personnel is identified and contact information shared? | Table 16 | | | | |
| **12** | Responsible for acceptance and handover is identified and contact information shared? | Table 17 | | | | |
| **13** | A system administrator is identified and contact information shared? | Table 18 | | | | |
| **14** | Remote backup configuration | Table 15 | | | | |

Table 19: Checklist

# 6 Abbreviations

**Dencrypt Server components**

| | |
|---|---|
| DCC | Dencrypt Control Center |
| DCS | Dencrypt Communication Server |
| DCM | Dencrypt Certificate Manager |
| DDB | Dencrypt Database |
| DPS | Dencrypt Provisioning Server |
| DSB | Dencrypt Server Birdge |
| DSS | Dencrypt Server System |

**General terms**

| | |
|---|---|
| API | Application Programming Interface |
| CA | Certificate Authority |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DCV | Domain Control Validation |
| DNS | Domain Name System |
| DMZ | De-Militarized Zone |
| IPv4 | Internet Protocol version 4 |
| NAT | Network Address Translation |
| MFA | Multifactor Authentication |
| RTP | Realtime Transport protocol |
| SCP | Secure Copy |
| SIP | Session Initiation Protocol |
| SMTP | Simple Mail Transfer Protocol |
| SMS | Short Message Service |
| SRTP | Secure Realtime Transport Protocol |
| SRV | Service Record |
| SSH | Secure Shell |
| STUN | Session Traversal Utilities for NAT |
| TCP | Transmission Control Protocol |
| TLS | Transmission Layer Security |
| UDP | User Datagram Protocol |
| VM | Virtual Machines |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| ZRTP | Zimmermans Realtime Transport Protocol |

## References

[1] Dencrypt, "Dencrypt Communication Solution - Support guide", www.dencrypt.dk/downloads.

[2] Dencrypt, "Dencrypt Communication Solution - Acceptance test".

[3] Dencrypt, "Dencrypt Connex- Operational User Guide", www.dencrypt.dk/downloads.

[4] Dencrypt, "Dencrypt Server System - Operational User Guide", www.dencrypt.dk/downloads.

# 7 Version history

| Ver. | Author | Date | Notes |
|---|---|---|---|
| 1.0 | SS | 25-06-2020 | Initial version in LaTeX based on DSS4.3.1 |
| 1.1 | SS | 07-08-2020 | Updated for CC DSS5.0 |
| 1.2 | SS | 19-08-2020 | Minor editorial corrections. |

# A Network port configuration and data flow

This appendix describes the configuration of external and internal networks port and the data flow for each of the server components. The following color-coding is applied:

- Red line: An ingoing data connection from the outside of the external firewall, i.e. from the internet to a Dencrypt local IP-address.
- Black line: An outgoing data connection from inside of the external firewall, i.e. from a Dencrypt Server to the internet.

In case an internal firewall is applied between Dencrypt servers, the following color-coding is applied:

- Green line: Data connection, which applies to RabbitMQ and the Dencrypt WebAPI services.
- Purple line: Data connection for a direct data service (MySQL, Minio S3).
- Yellow line: Data connections to synchronise user registration.
- Orange line: Data connections for VoIP clustering.

## A.1 Dencrypt Communication Servers

The ports and data flows for the two Dencrypt Communication Servers are identical.

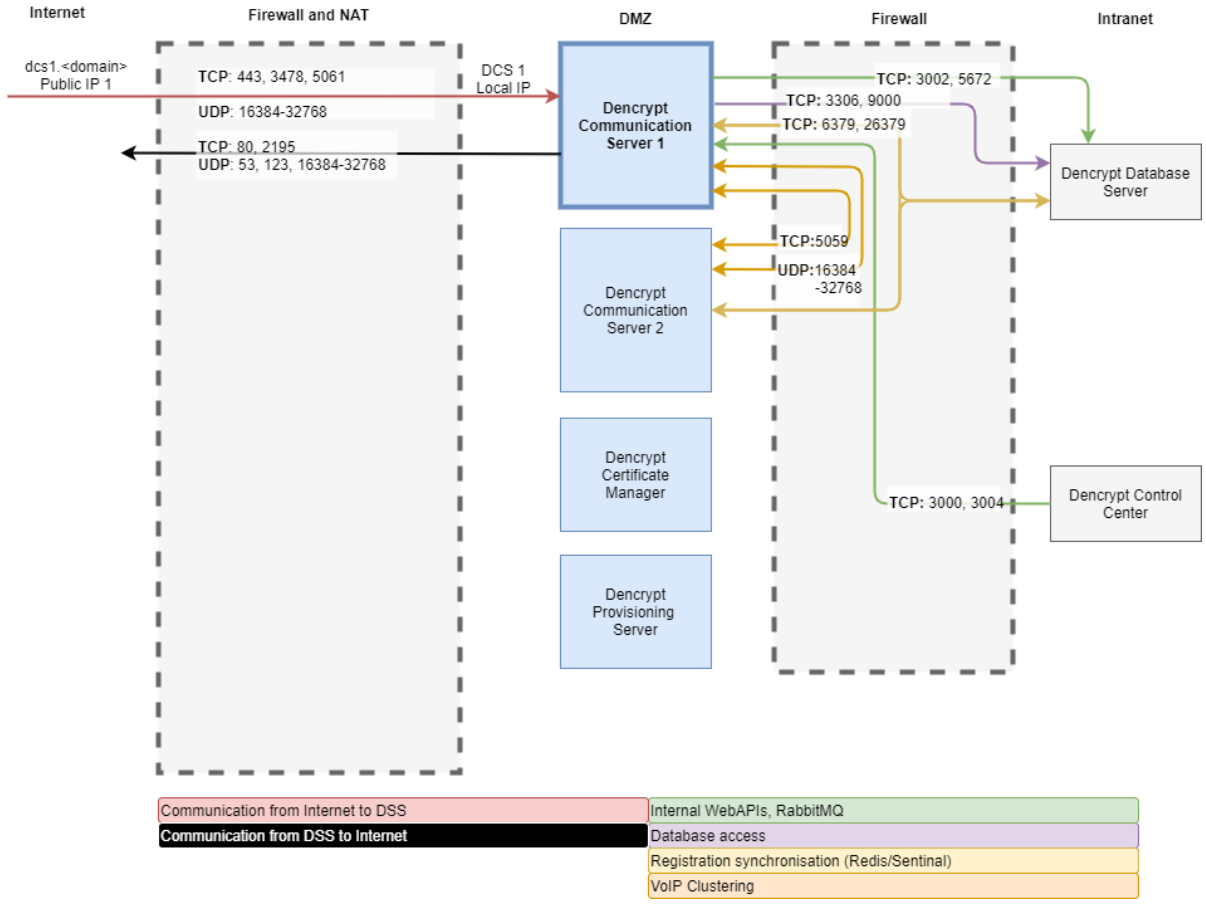


Figure 3: Ports and data flow for Dencrypt Communication Servers.

## A.2 Dencrypt Certficate Manager

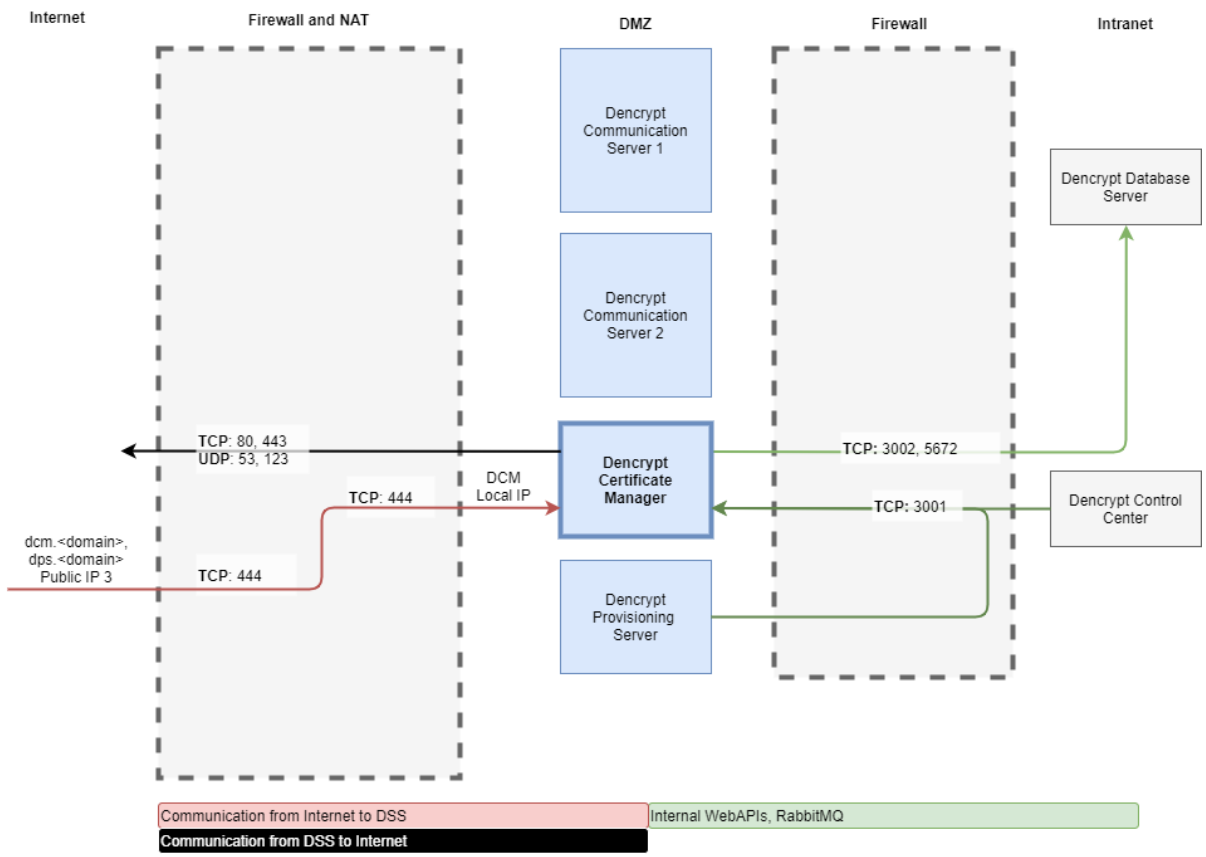


Figure 4: Ports and data flow for Dencrypt Certificate Manager.

## A.3 Dencrypt Provisioning Server

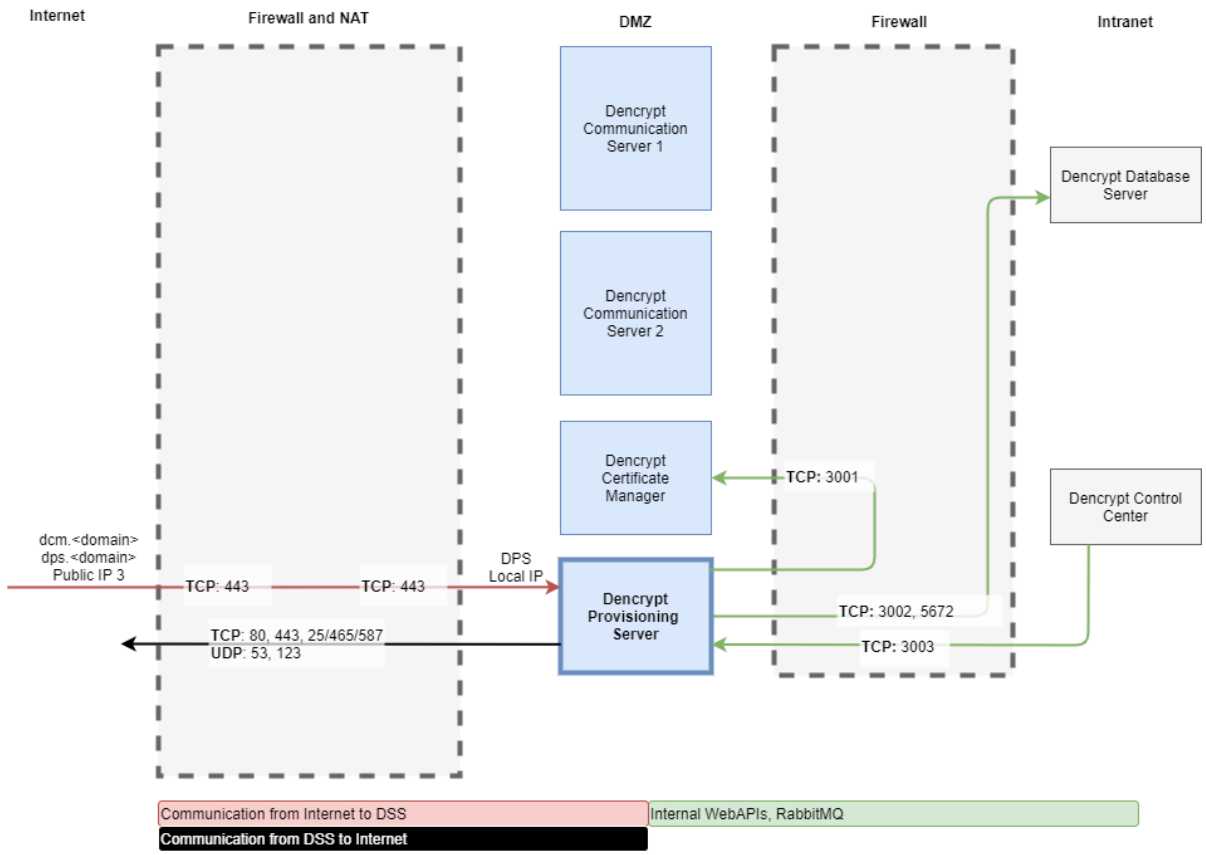


Figure 5: Ports and data flow for Dencrypt Provisioning Server.

## A.4 Dencrypt Database Server

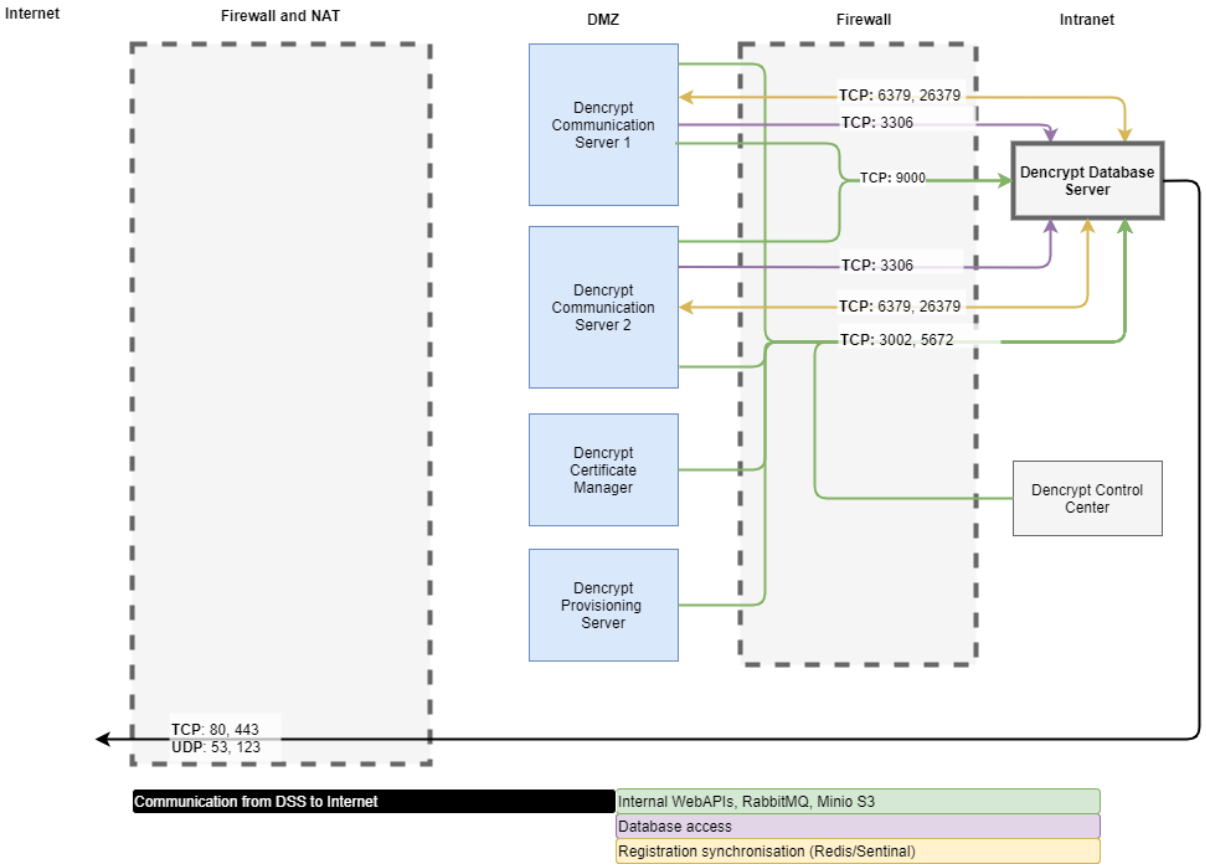


Figure 6: Ports and data flow for Dencrypt Database Server.

## A.5 Dencrypt Control Center

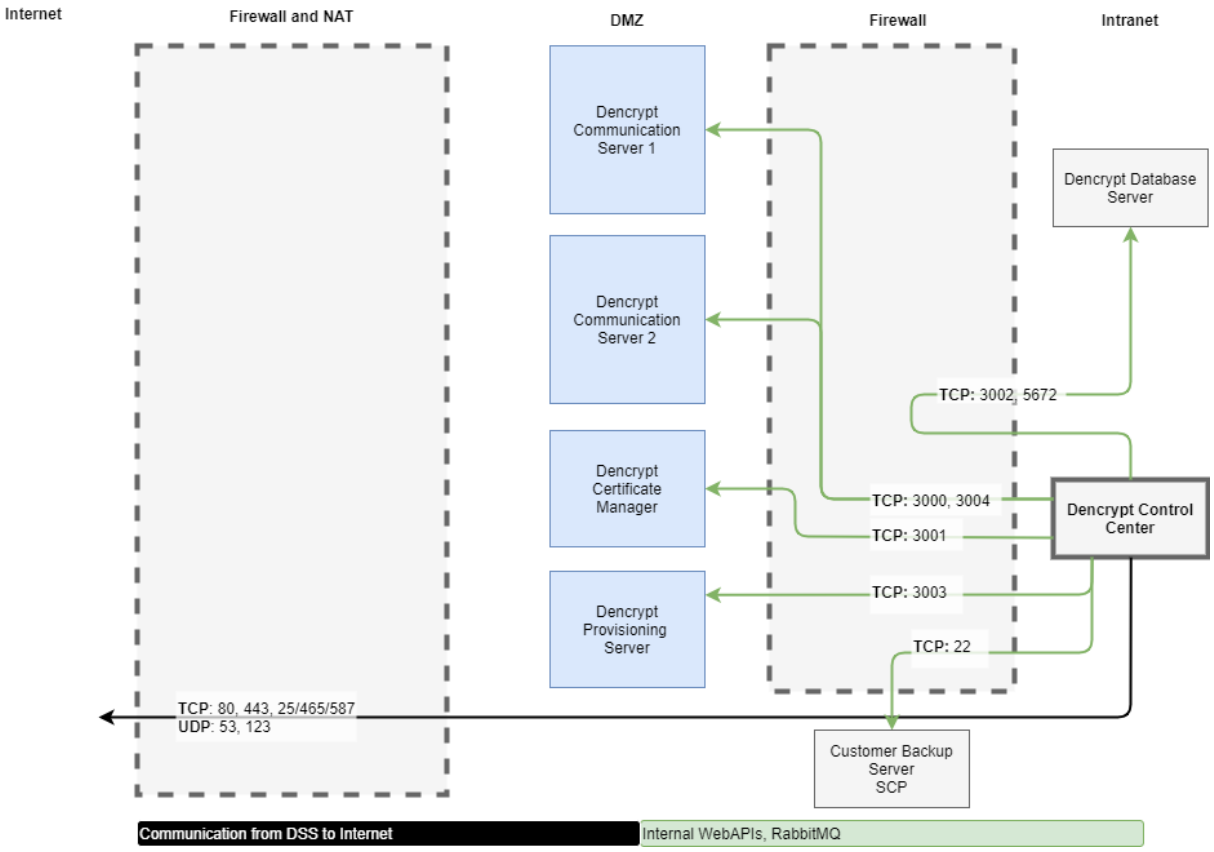


Figure 7: Ports and data flow for Dencrypt Control Center.