**Procurement for the  
Central Norway Health Region**

– Negotiated procedure –

**Case -/-**

The Norwegian Government’s Standard Terms and Conditions for IT-procurement SSA-T

Customer Technical Platform  
 v1.0

History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Initials | Date  dd.mm.yyyy | Comments/Changes |
|  | HMN |  | Invitation to Tender |
|  |  |  |  |
|  |  |  |  |

Content

[1 Introduction 5](#_Toc493166190)

[1.1 Technical environments used by Central Norway Health Region 5](#_Toc493166191)

[1.1.1 Test environment 6](#_Toc493166192)

[1.1.2 Production test environment 6](#_Toc493166193)

[1.1.3 Training environment 6](#_Toc493166194)

[1.1.4 Production environment 6](#_Toc493166195)

[2 OVERVIEW OF CURRENT LAB SYSTEMS 7](#_Toc493166196)

[2.1 Tieto Analytical Platform (ANP) 8](#_Toc493166197)

[2.2 Tieto RoS 8](#_Toc493166198)

[2.3 Tieto SymPathy 9](#_Toc493166199)

[2.4 Cerner DocuLive 10](#_Toc493166200)

[2.5 Tieto PAS 10](#_Toc493166201)

[2.6 Total Laboratory Automation TLA 11](#_Toc493166202)

[2.7 EVRY – Interactive Referral and Ordering (IHR) 12](#_Toc493166203)

[2.8 Tieto PM 12](#_Toc493166204)

[3 TECHNICAL PLATFORM SPECIALIST HEALTH CARE 13](#_Toc493166205)

[3.1 Overview 13](#_Toc493166206)

[3.2 Network 14](#_Toc493166207)

[3.2.1 Wide Area Network (WAN) 14](#_Toc493166208)

[3.2.2 Norwegian Health Network (NHN) 14](#_Toc493166209)

[3.2.3 Local Area Network (LAN) 14](#_Toc493166210)

[3.2.4 Wireless Local Area Network (WLAN) 14](#_Toc493166211)

[3.2.5 Virtual Local Area Network (VLAN) 15](#_Toc493166212)

[3.2.6 Firewall 15](#_Toc493166213)

[3.2.7 Remote access 15](#_Toc493166214)

[3.2.8 Protocols 15](#_Toc493166215)

[3.3 Servers 16](#_Toc493166216)

[3.3.1 Virtual servers 16](#_Toc493166217)

[3.3.2 Virtualization technology 16](#_Toc493166218)

[3.3.3 Physical servers 16](#_Toc493166219)

[3.3.4 Operating systems 17](#_Toc493166220)

[3.3.5 Databases 17](#_Toc493166221)

[3.3.6 Anti-virus 17](#_Toc493166222)

[3.3.7 Backup 17](#_Toc493166223)

[3.3.8 Monitoring 18](#_Toc493166224)

[3.3.9 SW distribution server 18](#_Toc493166225)

[3.4 Infrastructure services 18](#_Toc493166226)

[3.4.1 Active Directory (AD) 19](#_Toc493166227)

[3.4.2 Federation services (ADFS) 19](#_Toc493166228)

[3.4.3 PKI 19](#_Toc493166229)

[3.4.4 Email service 20](#_Toc493166230)

[3.5 SAN 21](#_Toc493166231)

[3.6 Platforms 23](#_Toc493166232)

[3.6.1 Data warehouse 23](#_Toc493166233)

[3.6.2 Integrations 24](#_Toc493166234)

[3.7 Emergency Systems 26](#_Toc493166235)

[3.8 Clients 27](#_Toc493166236)

[3.8.1 Hardware 28](#_Toc493166237)

[3.8.2 Basic Software 28](#_Toc493166238)

[3.8.3 Remote Control 29](#_Toc493166239)

[3.8.4 Software distribution 29](#_Toc493166240)

[3.8.5 Email client 29](#_Toc493166241)

[3.8.6 Anti-virus 29](#_Toc493166242)

[3.9 Client workspace 29](#_Toc493166243)

[3.10 Print and output management 30](#_Toc493166244)

[3.11 Identity and access management (IAM) 30](#_Toc493166245)

[3.11.1 User management 30](#_Toc493166246)

[3.11.2 User Logon 31](#_Toc493166247)

[3.11.3 Personal user 31](#_Toc493166248)

[3.11.4 Non personal user 31](#_Toc493166249)

[3.12 Test environments 31](#_Toc493166250)

Tables

[Table 1 External integrations 26](#_Toc493166251)

[Table 2 PC Client types 27](#_Toc493166252)

Figures

[Figure 1 Actors' overview (Norwegian Health Network (NHN)) 5](#_Toc493166253)

[Figure 2 HMN LAB Integrations 7](#_Toc493166254)

[Figure 4 Overview ANP 8](#_Toc493166255)

[Figure 5 Overview RoS 9](#_Toc493166256)

[Figure 7 Overview SymPathy 10](#_Toc493166257)

[Figure 8 TLA concept 11](#_Toc493166258)

[Figure 9 Specialist health service overview 13](#_Toc493166259)

[Figure 10 Virtual LAN 15](#_Toc493166260)

[Figure 11 Server virtualization 16](#_Toc493166261)

[Figure 12 Active Directory 19](#_Toc493166262)

[Figure 13 Email service 20](#_Toc493166263)

[Figure 14 High-End SAN 21](#_Toc493166264)

[Figure 15 Mid-Range SAN 22](#_Toc493166265)

[Figure 16 Data Warehouse 23](#_Toc493166266)

[Figure 17 Integration overview 24](#_Toc493166267)

[Figure 18 Internal and external integrations 25](#_Toc493166268)

[Figure 19 Overview BizTalk 26](#_Toc493166269)

[Figure 20 Print Concept 30](#_Toc493166270)

# Introduction

This document intends to give a short overview of the Customers’ existing technical platform.

To ensure high availability and optimal day-to-day operation the customer has emphasizes on standardizing technical infrastructure and operating systems. By standardizing and ensuring that systems are up to date, the operation, support and security level of the ICT-systems is enhanced.

The figure below provides a brief overview of the technical platform interconnecting the different actors in the laboratory discipline in the Central Norway Health Region.

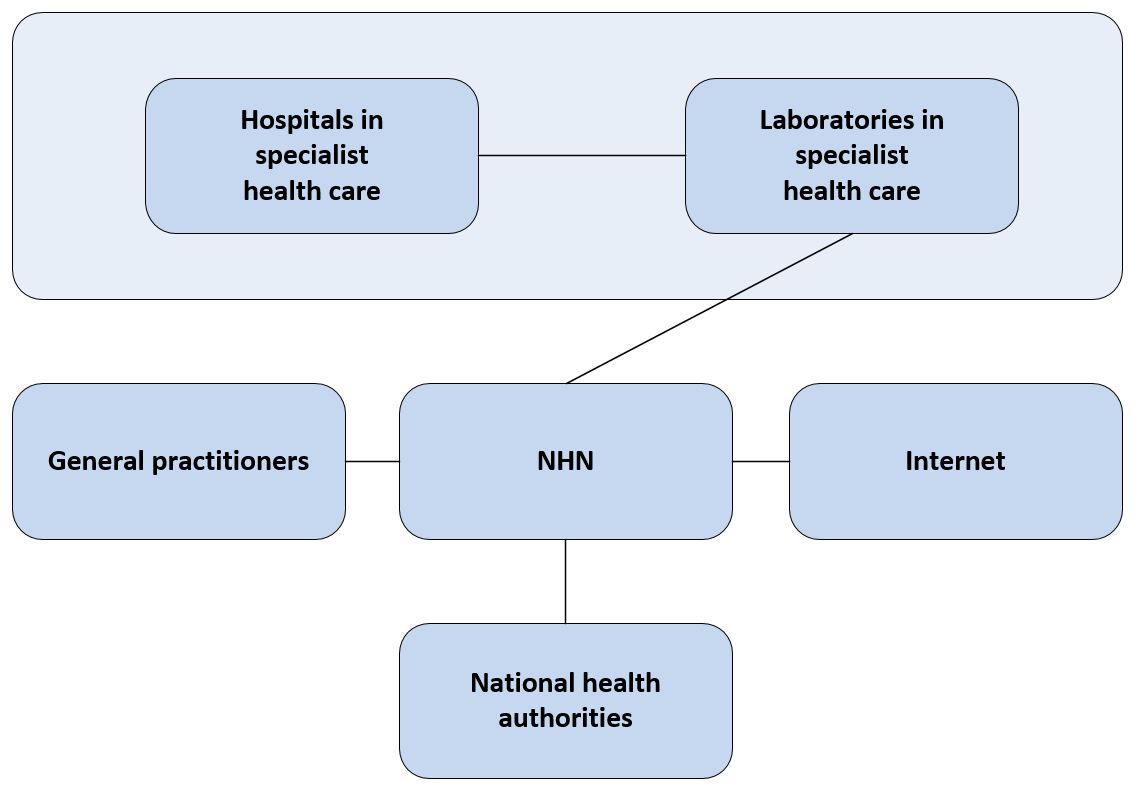


Figure 1 Actors' overview (Norwegian Health Network (NHN))

## Technical environments used by Central Norway Health Region

The Customer uses four separate environments for staging and production. All staging environments are based on virtualised server infrastructure and the configuration, patch level and versioning of these environments reflect the production environment. The production environment consists mostly of virtualised servers, but some solutions with special needs or extensive workload use physical servers.

### Test environment

The test environment is used to test setup and configuration of new solutions or upgrades of existing solutions. After setup or upgrade the solutions are tested for failures or new functionality. Anonymised production data are preferred to use during testing. The test environment is only used for testing. When the solutions have passed the test requirements they may be transferred to the production test environment and the training environment.

### Production test environment

The production test environment (pre-production environment) is used to verify that a solution will function in a production environment. When solutions are transferred to production test they now use production data. The environment is used by several resources to see how the solution is functioning in real life operation. After the production test have been completed the solutions is ready to be implemented in the production environment.

### Training environment

The training environment is used in courses and self-teaching. This environment can also be used by users who want to check out new functionality and features before used in production with real life data.

### Production environment

The production environment is where all solutions used by the Customer operate. The rest of this document will contain detailed information about standards and solutions used by the Customer.

# TECHNICAL PLATFORM SPECIALIST HEALTH CARE

## Overview

The specialist health care operates a technical platform for the following actors in the health service:

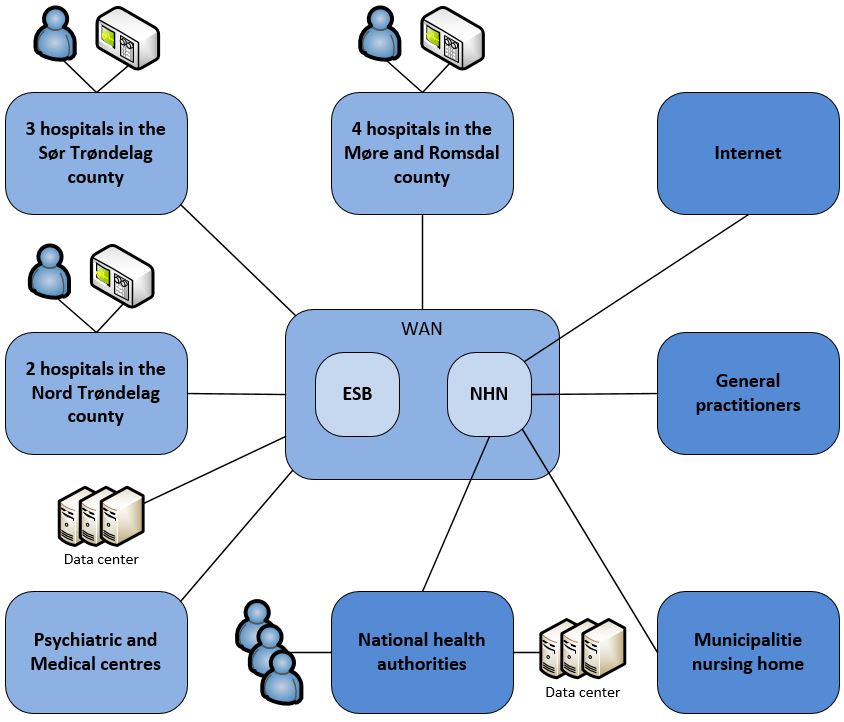


Figure 9 Specialist health service overview

The specialist health service operating the hospitals connects to the NHN and integrates the national, GP and municipality health service, mainly by message exchange.

An Enterprise Service Bus (ESB) orchestrates the message exchange between the parties in the health sector.

A high availability datacenter, distributed on two different physical locations in Trondheim, provides the technical infrastructure necessary to distribute shared health services to the other actors in the health sector.

## Network

### Wide Area Network (WAN)

The WAN infrastructure consist of a large number high capacity and redundant leased lines (fiber and other technologies) from different communication vendors in the market. Line capacity and redundancy varies from site to site according to the size of the organization to interconnect.

A high capacity ***NHN*** connection provides a secure and functional electronic message exchange with the other actors in the health sector and a secure Internet connection.

Cisco technology forwards and routes the IP based network traffic between sites in the health service.

### Norwegian Health Network (NHN)

***NHN*** (owned by the Ministry of health and care services) interconnects the Norwegian health sector and supplies common application services as well as an Internet connection to the connected participants.

### Local Area Network (LAN)

The LAN infrastructure comprises of high capacity lines (1 Gb or higher) and the local network traffic are routed and forwarded by Cisco technology, based on a standard edge, distribution and core layered switch architecture.

Cisco edge switches are of type WS-3560, WA-3560E, WA-3650, WS-C4500-E and 3650-48PD. Switches used by servers are of type Nexus5000/2000. Cisco core switches/routers are of type WS6500, WS6800 and Nexus7000.

### Wireless Local Area Network (WLAN)

The Hospital campuses broadcast wireless networks for managed clients to automatically connect to with a uniform and enterprise wireless network name (SSID). A guest wireless network is also available for unmanaged clients.

The wireless network infrastructure comprises solely of Cisco technology implemented as a centralized architecture, giving the central high-available master Wireless LAN Controllers (WLC) the mandate to control the distributed slave access points (AP).

Managed PC clients have to perform a successful IEEE 802.1x machine authentication to get access to wireless networks.

Cisco APs are of type Aironet 3700,3600,3500,1242 and the WLC’s of type Cisco WiSM.

### Virtual Local Area Network (VLAN)

Virtual LANs partitions the physical network into different logical network zones. The network traffic flows in a physical network infrastructure partitioned in different logical network zones, to ensure a secure and functional handling and transport of different data classes.

PC clients get access to logical networks zones by performing a successful IEEE 802.1x authentication and a dynamic VLAN assignment.

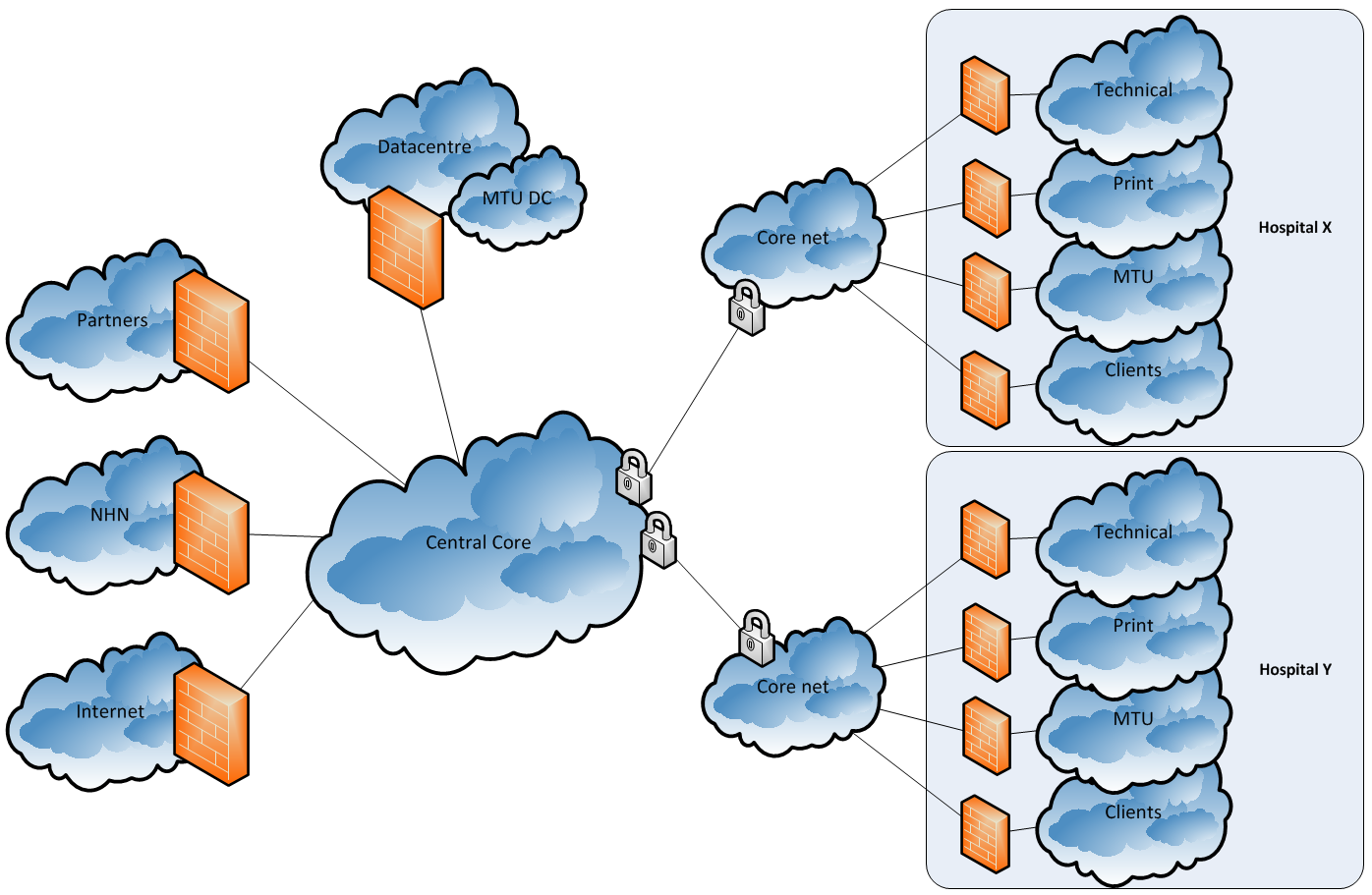


Figure 10 Virtual LAN

### Firewall

Firewalls are managing and controlling the IP network flow, ensuring an intended network flow between logical network zones. A central management station is managing and distributing the firewall rules.

All network traffic forwarded through and blocked by the Firewall is logged.

The Firewall technology is mainly Cisco ASA on WISM module and Check Point.

### Remote access

Remote access for employees in the specialist health service uses Microsoft Direct Access, which requires support for IP version 6.

A Citrix based remote access solution enables remote access for administrators and vendors.

### Protocols

The basic communication protocol is IP version 4.

## Servers

### Virtual servers

The central health region has standardized on virtualized hardware. The grade of virtualization is more than 90% (about 1300 servers). Windows servers are running on VMWare ESXI.

### Virtualization technology

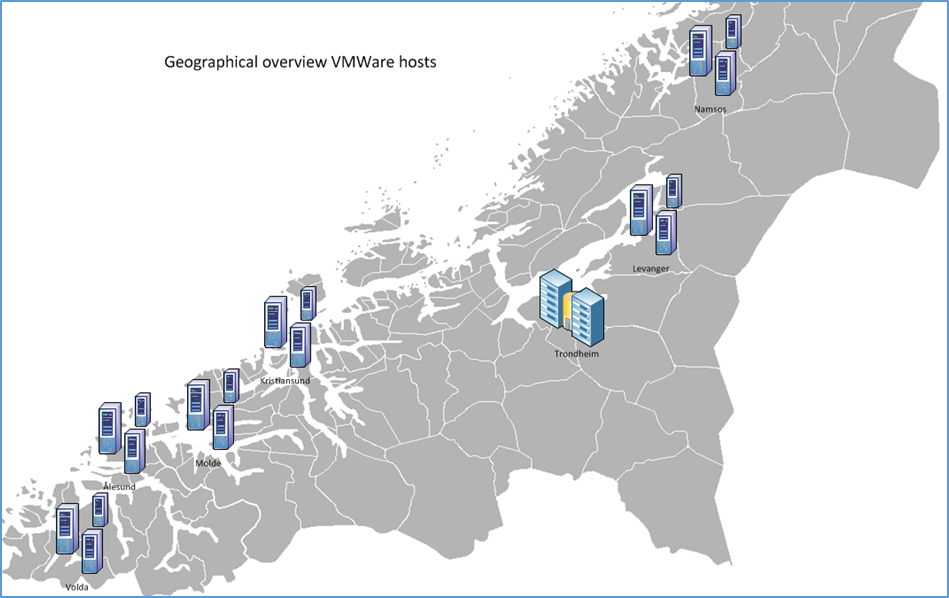


Figure 11 Server virtualization

The production environment comprises of several VMWare farms located at the hospitals, in different geographical locations. The VMWare farms comprises of a total of 50 ESXi hosts and approximately 30 of them are located at the main datacentre in Trondheim.

A VMWare VDI farm comprises of 64 ESXi hosts scaled to publish approximately 6.000 virtual clients.

### Physical servers

Several physical HP NonStop servers run the patient administrative system, laboratory systems and a shared authentication solution for several other systems.

SQL servers hosting consolidated database instances are running on physical server hardware due to extensive workload.

### Operating systems

The standard server operating systems is Microsoft Windows servers. The standard version of Windows server is at the moment 2012 R2. Standard server operating systems are regularly upgraded to meet service and support agreements.

HP NonStop servers are running NonStop operating system.

Web servers are mainly Microsoft Internet Information Server (IIS) version 7.5 and 8.5.

### Databases

The specialist health service is standardizing on Microsoft SQL servers configured as a Failover Clustered environment, comprising of several database instances in each cluster. The different SQL instances supports a consolidated production environment.

SQL versioning today is standardized on SQL 2012r2 and SQL 2016. SQL versioning is regularly updated in line with Microsoft support timeframe. This is done to maintain operational support and stable operation.

Separate SQL instances or dedicated physical/virtual database server are allocated for systems with special needs or extensive workload.

Some databases are running on Oracle ver. 12c RAC. Oracle is running on top of Windows server 2012 R2.

Databases for laboratory systems and patient administrative systems are running on HP NonStop servers. The HP NonStop servers are located in two datacentres. One server is handling the production environment, and the other one act as a disaster server. The disaster server is always in sync with the production environment. The synchronisation of files, applications and databases is handled through HP NonStop Remote Database Facility (RDF) and HP AutoSYNC. Transactions integrity, database consistency and database/transaction recovery is safeguarded through HP NonStop Transaction Management Facility (TMF).

### Anti-virus

Windows servers are running antivirus software and the Windows firewall is enabled.

### Backup

Snapshot technology performs backup and restore of data in the VMWare environment. Accordingly, NetBackup performs backup and restore of data on physical servers.

Backup and restore of databases are performed by RMAN for restore Oracle databases and SQL agent job (T-SQL) on file share (Data Domain) for Microsoft SQL databases.

### Monitoring

A dedicated team is developing and maintaining monitoring solutions for servers and network.

#### Network

* SPLUNK monitor data traffic by performing correlation of logs from network and firewall devices, to detect issues. SPLUNK is also used to create monitoring dashboards for different services
* Network Node Manager (NNM) monitors all network nodes, both wired and wireless
* Cacti is used to monitor and log network traffic and load
* NeDi keeps track of the relationships between VLANs, switch ports and connected nodes
* Websense monitor and control web traffic

#### Server

* SPLUNK monitor services by performing correlation of logs from servers, to detect incidents
* Foglight perform real time monitoring and trending of VMWare environments
* In-house developed database monitoring solution support custom needs for monitoring, reports and trending. This solution triggers SMS alerts based on predefined thresholds for system events.
* Microsoft System Center Operations Manager (SCOM) is the standard monitoring suite for servers. SCOM is custom configured to fit different needs for monitoring of services and systems
  + Dashboards are used to display customized heat maps for different monitoring needs suited for different purposes
  + Event management generating SMS alerts based on custom configured system triggers.
* The Riverbed performance management suite perform monitoring, debugging and trending of network traffic and performance related issues

### SW distribution server

Servers follow Microsoft best practice for patching and updating. Microsoft System Center Configuration Manager (SCCM) perform automated server patching.

Automated SCOM functionality patches approximately 90% of the servers and the remaining servers are patched manually due to special needs.

## Infrastructure services

Microsoft Active Directory forest contains ten domain controllers with functional level 2012 R2. The domain controllers are running on Windows server 2012 R2.

Four of the domain controllers are located at the data centres in Trondheim. The remaining domain controllers are located at the other hospitals in the region.

### Active Directory (AD)

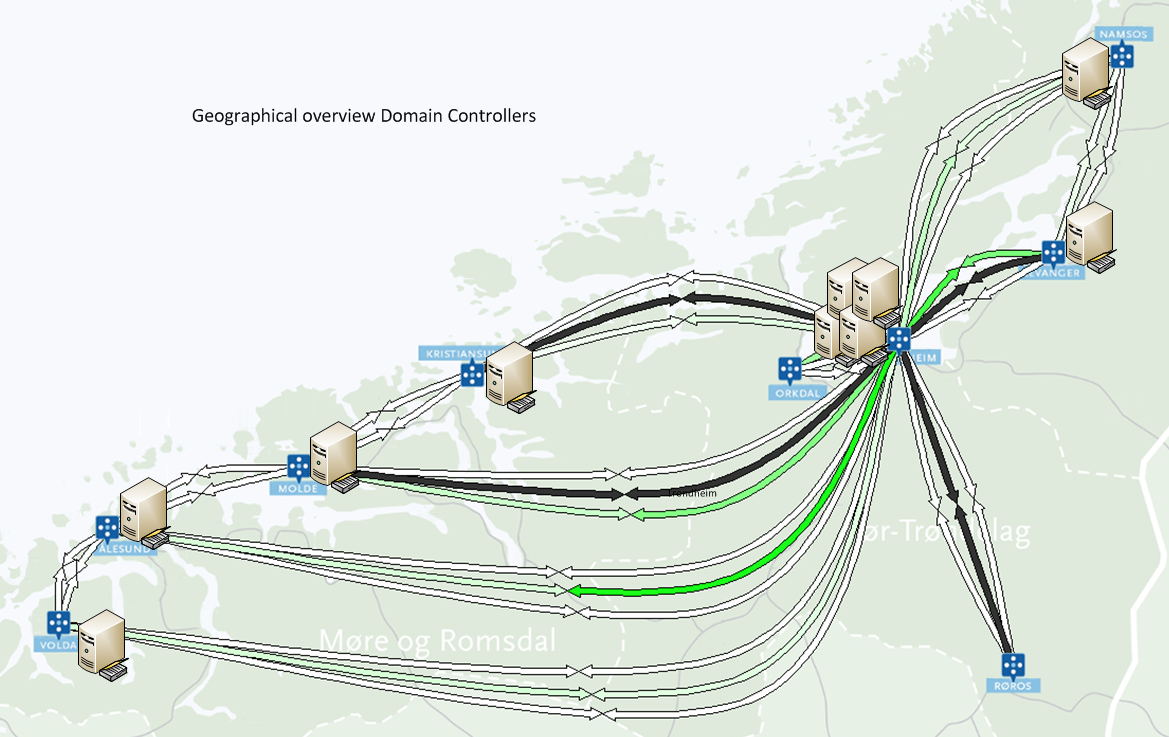


Figure 12 Active Directory

### Federation services (ADFS)

Active Directory Federation Service has been implemented to enable access to remote web application services for local users and access to local web application services for remote users.

### PKI

An intermediate PKI service issues certificates to clients, servers and users.

NHN is hosting the root CA and the revocation information is published in the NHN network. The Microsoft AD CS intermediate CA is managed by the specialist health service and the local revocation information is published in AD and to a Certification Revocation List (CRL) web server.

### Email service

The email solution is Microsoft Exchange 2010 SP2, on top of a Windows server 2008 R2 running on virtualized server infrastructure.

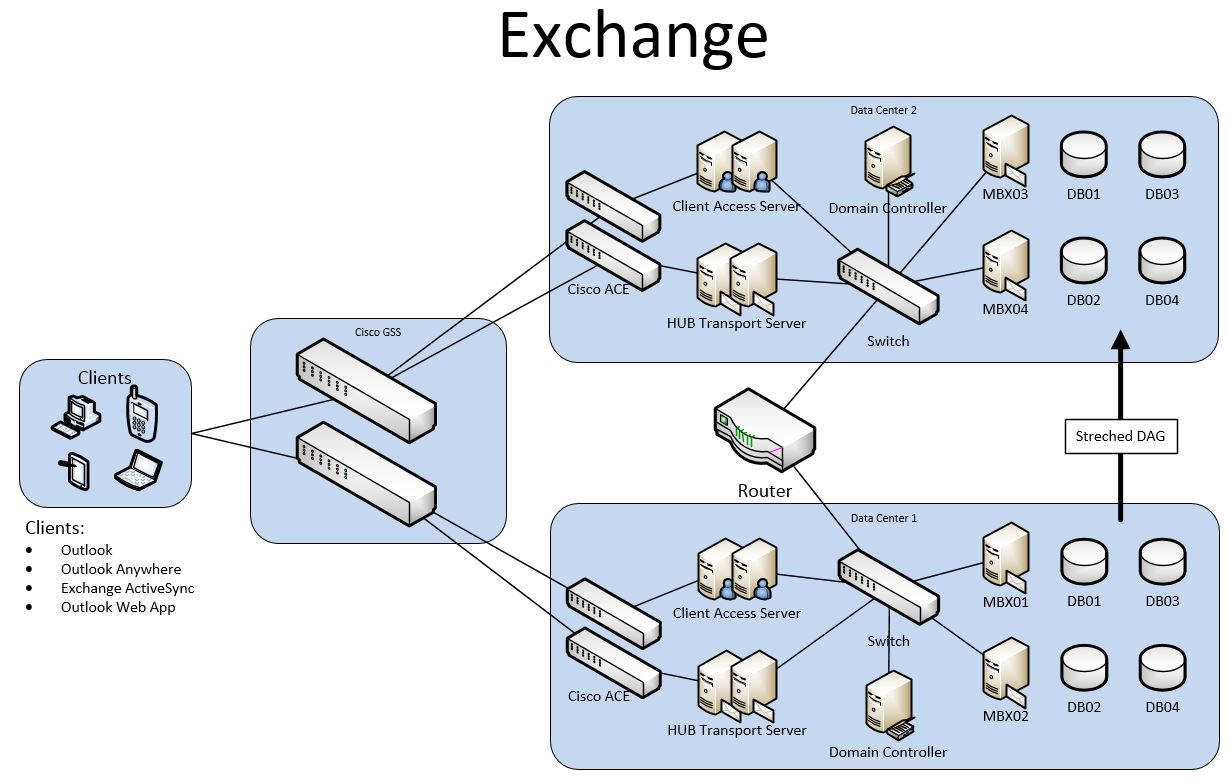


Figure 13 Email service

## SAN

The high-end quality storage solution is Hitachi VSP G1000, configured with a synchronous mirroring between datacenters over a dedicated fiber network.

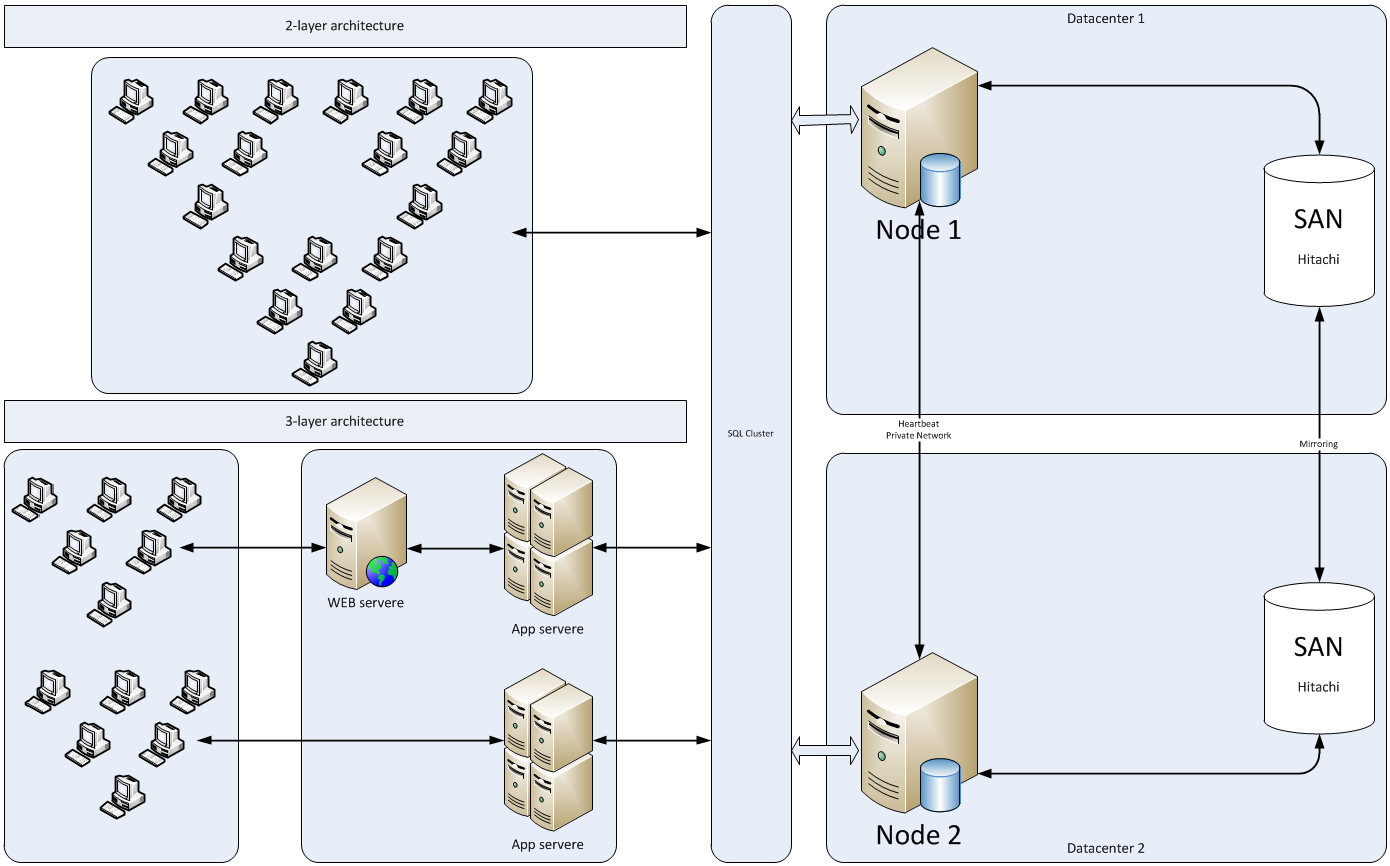


Figure 14 High-End SAN

The mid-range quality storage solution is NetApp SAN configured with asynchronous mirroring every hour over a dedicated fiber network.

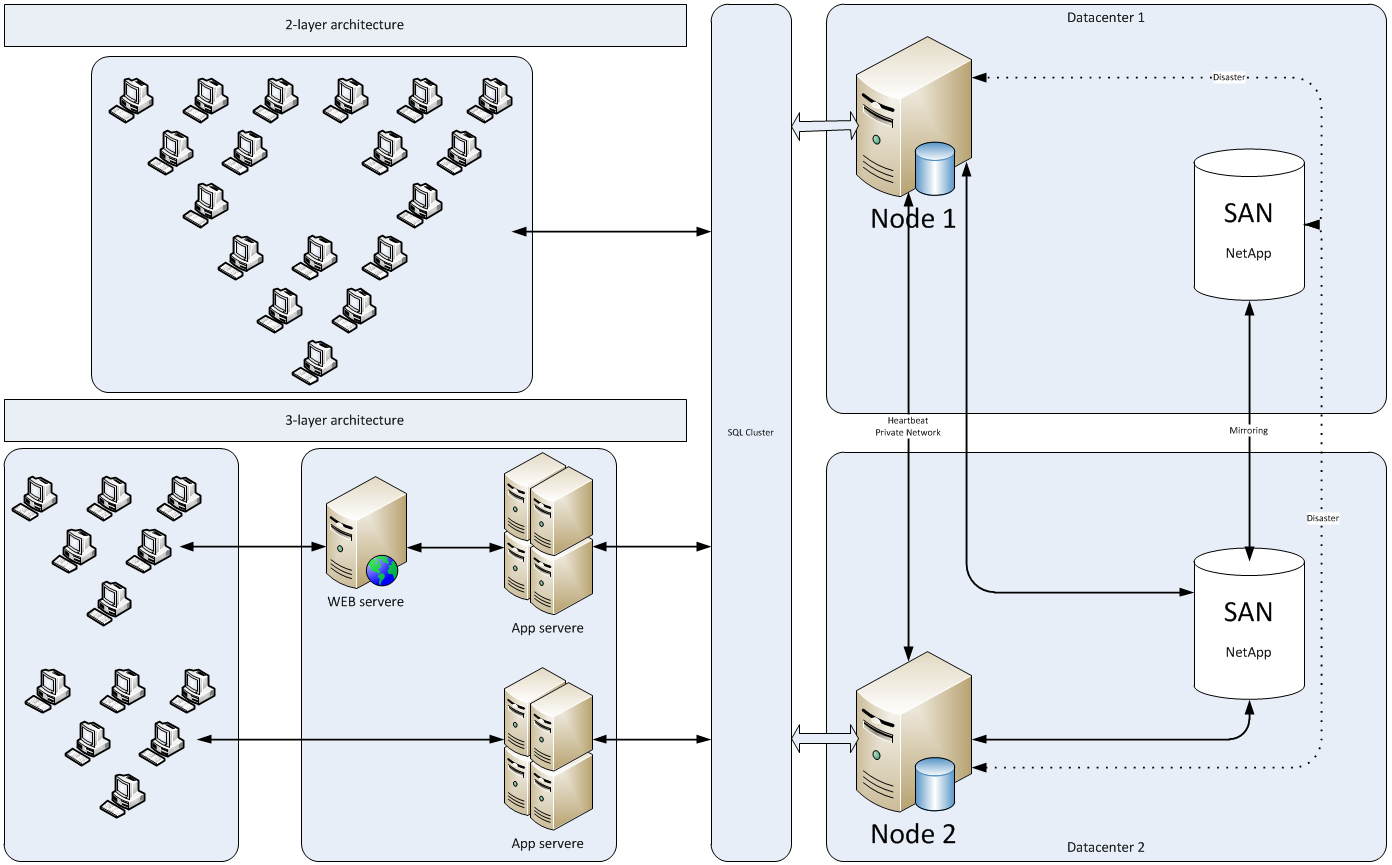


Figure 15 Mid-Range SAN

Data Domain from EMC is used as backup storage, currently running DD2500 and DD670. It is worth mentioning that it is an ongoing effort to implement new NetApp SANs with all flash storage. There is also ongoing planning to expand and convert the vSAN operational environment to all flash storage.

## Platforms

### Data warehouse

Figure below gives an overview of the current data warehouse solution.

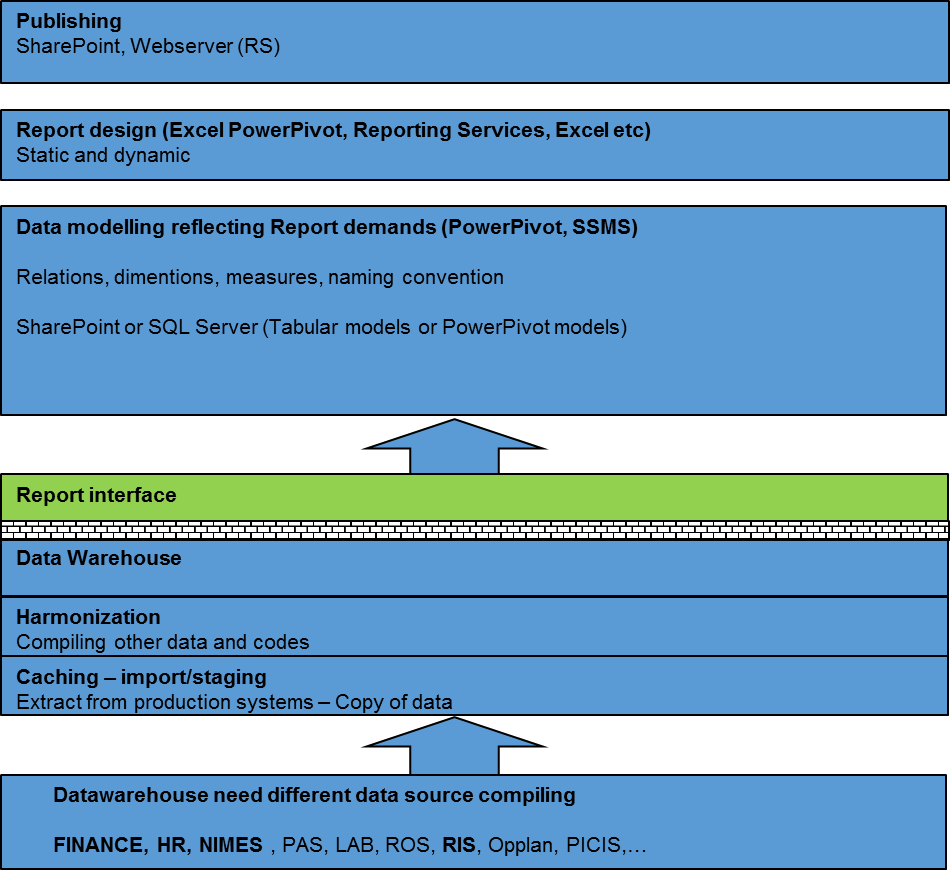


Figure 16 Data Warehouse

Report Interface basic information (marked green) is extracted from various back-end systems.

### Integrations

Overall integration overview including built-in and ***ESB*** integrations:

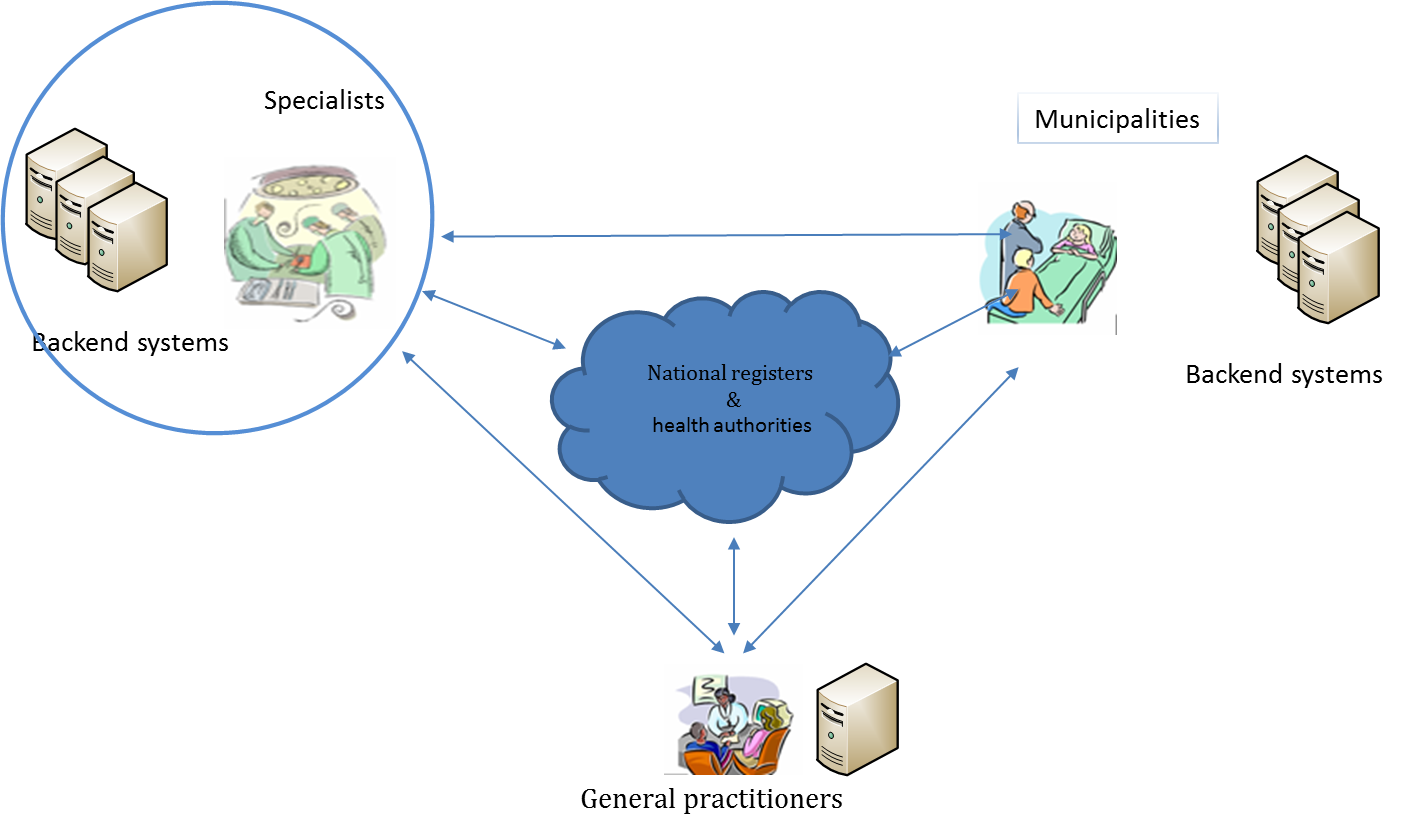


Figure 17 Integration overview

The enterprise service bus (ESB) consist of a Microsoft BizTalk 2013 R2 integration services, providing internal and external integrations. The latter integrates (a blue square in Figure 12 below) with the National health authorities, municipalities, general practitioners (GP) and partners/actors in other health regions in Norway.

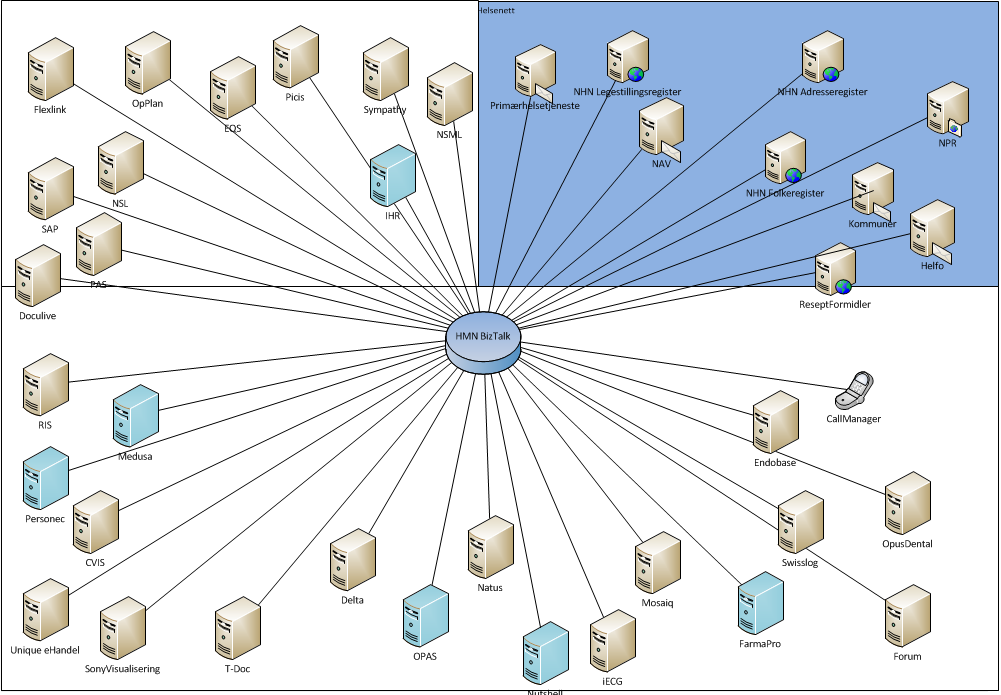


Figure 18 Internal and external integrations

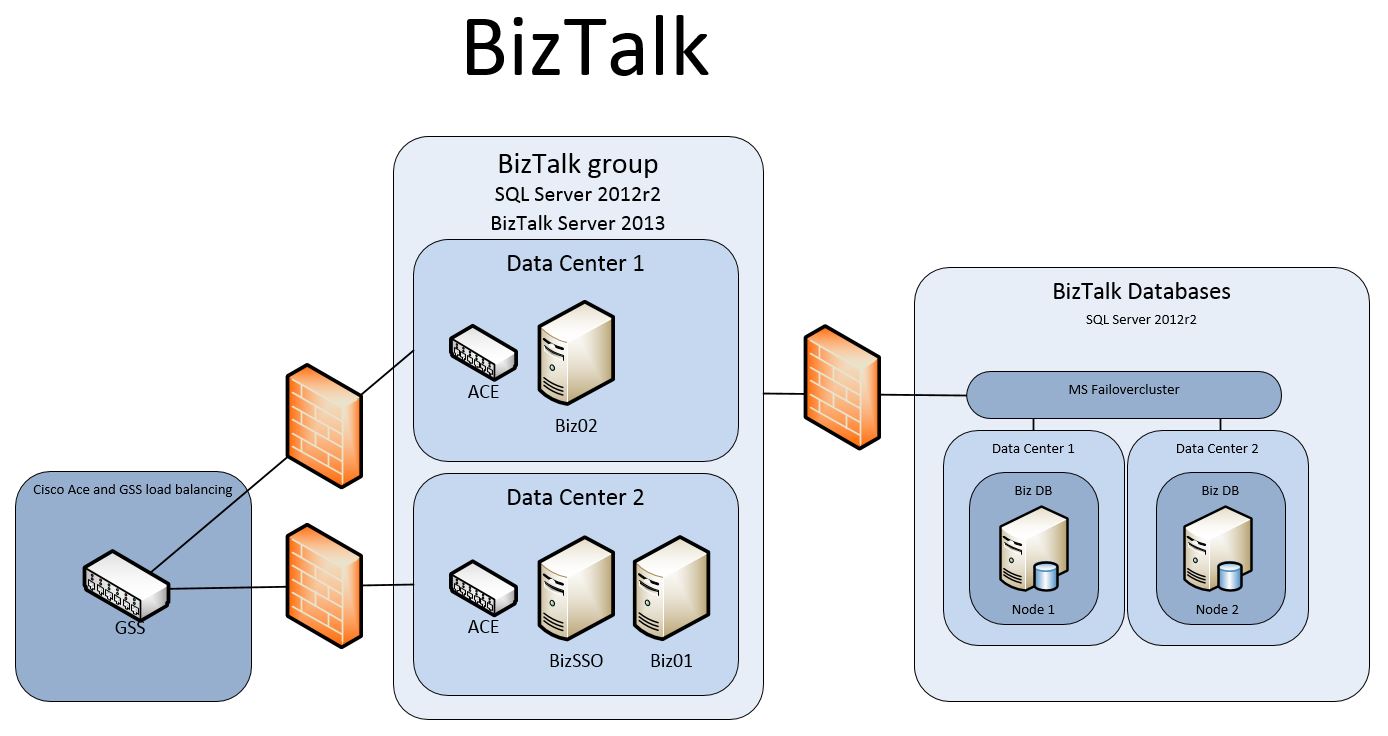


Figure 19 Overview BizTalk

Internal integrations provide data exchange and transformation utilizing Netapp File Transfer, SQL, MSMQ and Web services.

External integrations provide data exchange and transformation utilizing SMTP/POP3, FTP/SFTP and Web services.

Table 1 lists examples of external integrations.

|  |  |  |  |
| --- | --- | --- | --- |
| Sender | Receiver | Message Content | Comment |
| PAS | NAV/***The Norwegian Health Economics Administration (HELFO)*** | BKM (refunds) | National format |
| EPJ | Reseptformidleren (national prescription) | Prescription refund | National format |
| GP | Specialist health services | IHR Request | National format |

Table 1 External integrations

## Emergency Systems

The specialist health service contingency management uses an external system (HelseCIM) operated by national contingency services to manage an emergency.

## Clients

There are defined three different types of clients:

* Standard
  + Standard Windows 7/10 client intended for regular clinical and administrative use, where the users logs on using a personal smart card. These types of clients are typically used where there are only one or two users sharing a computer, for example in an office.
* Spesial
  + Standard Windows 7/10 client with automatic system user logon at startup intended used as interface clients connecting to analysis instruments or applications with special requirements.
* Sprint
  + Locked down Windows 7/10 installation, used as thin client endpoints for the Virtual Desktop Infrastructure (VDI). These clients are typically used where there are multiple users sharing the computer, for example in the clinics and wards. Users logs on/reconnects using a personal smart card and disconnects from the session when the smart card is removed.

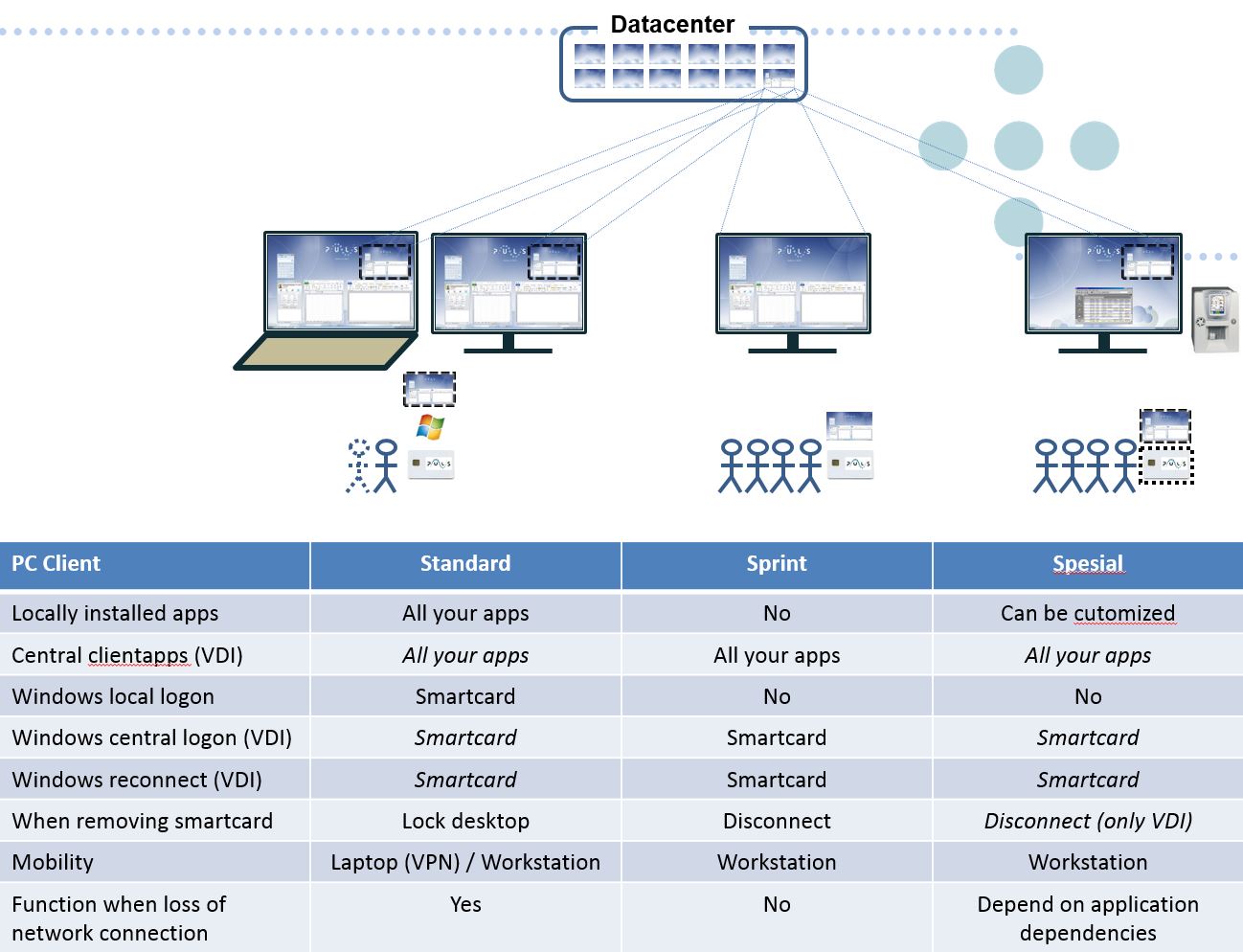


Table 2 PC Client types

The Virtual Desktop Infrastructure is built on VMware Horizon View, and is scaled for 4000 concurrent users. VDIs are mainly used by clinical users with the need to log on to multiple computers on multiple locations during a workday. By disconnecting/reconnecting to the virtual desktops, they save time and get to keep their session when they move from computer to computer.

Desktop pools are floating linked clones that refreshes once a week. Golden image is a Windows 7/10 installation, with a minimum set of basic applications and middleware installed, and best practice tuning for running in a VDI environment.

Laptops use standard a local user profile, and have enabled functionality for offline sync of documents and email. Remote access to the specialist health service network from a laptop is provided by Microsoft Direct Access.

Clients are running System Center Endpoint Protection and the local Windows Firewall is enabled, centrally managed via Group Policy (GPO). Patching and updates done according to Microsoft best practice recommendations to enhance security and stable operation. PC clients are patched on a monthly basis (Windows, Office, Adobe Flash, .Net, Silverlight, AV, IE) and virtual clients once every third month.

### Hardware

The region has a standardized client platform based on Windows 7 SP1 x64, where approximately 20% are laptops and 80% are desktops, 17000 physical clients in total. Hardware lifecycle for PCs are 4 years. It is worth mentioning that it is an ongoing effort planning to switch from Windows 7 to Windows 10 client operating system.

Mobile devices and tablets are not in use in the clinical work today, the only service at this time provided to these devices are email synchronization.

### Basic Software

The centrally managed clients is based on a Microsoft SCCM distributed client image and Active Directory GPO configuration.

The following software is a part of the image, and available from all types of clients:

* Microsoft .Net Framework 4.6.1
* Microsoft Silverlight 5.1.4
* Microsoft Office 2010 and 2016
* Microsoft Internet Explorer 11
* Skype® for Business 2016
* 7-Zip 15.14
* Adobe Flash Player (IE) 20
* Adobe Reader DC
* Adobe Shockwave Player 12.1
* Java 6 Update 45
* Java 8 Update 74
* PDF Creator 2.3.0
* Citrix Online Plug-in 12.1.4
* Microsoft MSXML 4.0 SP3
* VLC Media Player 2.2.0
* Microsoft Virtual C++ 2005-2015 Redistributable packs.
* Net iD 6.4.0
* RES Workspace Manager 2014 SR2
* Netop Remote Control 12.20

### Remote Control

Netop Remote Control 12.20 is used to handle remote of clients.

### Software distribution

Applications are distributed to computers/users either as a thick installed application or virtualized with Microsoft App-V. Software packages are streamed from a distributed file system (DFS), where a local copy of all packages are stored for all hospitals.

Security groups in Active directory grants users access to applications and builds collections (machine) for distribution in SCCM.

The goal is to App-V virtualize as many applications as possible and currently approximately 80% of all applications are virtualized and published as App-V applications. Microsoft SCCM distributes and installs applications that are not App-V virtualized.

### Email client

The standard email client is MS Outlook 2010. It is worth mentioning that it is an ongoing effort planning to switch from Windows 7 to Windows 10 client operating system. Once this change is implemented, the new standard email client will be MS Outlook 2016.

### Anti-virus

Microsoft System Center Endpoint Protection. It is worth mentioning that it is ongoing planning to switch from Microsoft System Center Endpoint Protection to Trend Antivirus solution in the future.

## Client workspace

RES Workspace Manager handles management of the user environment and profile data. Application shortcuts, user settings and print- and drive mappings are distributed to the user based on the user and client context at the time of logon or reconnect.

On desktops and virtual clients, a custom created mandatory user profile is used, which is deleted from the client when the users logs off. User profile settings are being preserved using RES Workspace manager and are applied to any client the user logs on.

## Print and output management

Print is delivered by the Microsoft Windows Printing service in cooperation with a Follow-Me print solution manufactured by Safecom.

Windows Server 2008 R2 print servers are installed on each hospital and only with Windows 7/10 x 64 print drivers installed.

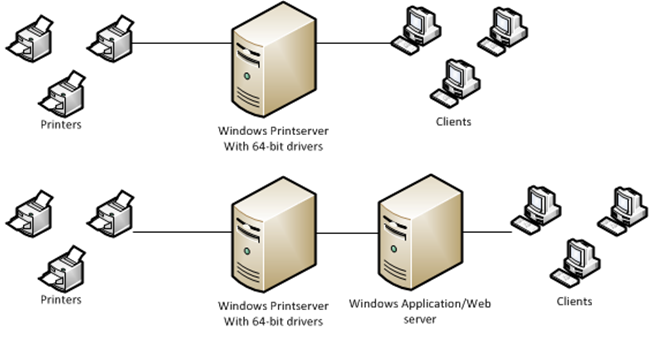


Figure 20 Print Concept

There are approximately 3.500-4.000 network printers and 2.000 locally connected printers, in a variety of makes and models.

RES Workspace Manager connects the printers to the user sessions, based on the physical location of the client. Printers and clients are organized into zones, where all clients in the zone get all associated printers, connected at user logon.

## Identity and access management (IAM)

Two IAM solutions are managing the user directory. A proprietary solution developed and maintained by HMN is working in parallel with the Microsoft Forefront Identity Manager (FIM).

Both solutions maintain identity data in Active Directory. The proprietary IAM solution grants users access to applications.

It is worth mentioning that it is an ongoing planning to move all identity and access management to FIM in the future.

### User management

The human resource (HR) system Tieto PRS is managing employee identities. Student identities are managed by the HR system operated by Norwegian University of Science and Technology (NTNU) and through integration populate AD with user objects.

User identities from HR systems are populated as user objects in AD through FIM and the proprietary IAM solution. For some hospitals the HR systems populate only AD and the IAM solution.

### User Logon

Users log on to a Windows domain and authenticates using a personal certificate stored on a smartcard. Applications authenticate users in different ways:

* Application defined username and password
* AD defined username and password
* Integrated authentication provides Single Sign On

### Personal user

All end users are assigned a dedicated user object in AD. Applications not integrated with AD are managing built in user directories.

Users granted administrative privileges are allocated a separate administration user object.

### Non personal user

Applications and system services use privileged system users defined in AD, to logon to the Windows domain.

Clients of type Spesial logs on the Windows domain with a dedicated system user at start-up.

## Test environments

Dedicated test users are defined in the test environments, which are used for testing of patches, new builds and new integrations.

HP ALM provides functionality for test management.