

The Internet-based Health Data Net

Version 1.0

**The Internet-based Health Data Net
Version 1.0**

©UNI•C December 2003

By Martin Bech and Ib Lucht

Contents

| | |
|---|----|
| 1 Introduction | 2 |
| 1.1 Summary | 2 |
| 1.2 Aim..... | 2 |
| 1.3 Stakeholders | 3 |
| 2 The Health Data Net | 3 |
| 2.1 Status on beginning operations in August 2003..... | 4 |
| 2.2 Subscribers to the Health Data Net in August 2003..... | 4 |
| 3 Technical solution | 4 |
| 3.1 The technical solution..... | 5 |
| 3.2 VPN, GRE, IPSec, Internet connection, Agreement system, Summaries and operation status, Security | 5 |
| 3.3 IP addresses | 7 |
| 3.4 DNS..... | 8 |
| 3.5 edi-mail..... | 9 |
| 3.6 Video | 10 |
| 3.7 Web mail | 11 |
| 4 References | 12 |
| 5 Illustration of the Health Data Net..... | 14 |

1 Introduction

0.0 Summary

In implementing the practical realization of the MedCom Internet strategy, UNI•C carried out a preliminary technical study of the connection of the existing data net within the health sector through the use of Internet technology.

As a step in the technical clarification of possible designs for the Internet-based Health Data Net, UNI•C has, in cooperation with MedCom, conducted a round of interviews with a large number of stakeholders to cast light on the possibilities and/or limitations which exist with regard to connecting the current data nets.

The preliminary study resulted in a proposal to start a pilot project on establishing an Internet-based Health Data Net based on virtual connections on the Internet via a central node. The idea was that stakeholders should use existing connections to the Internet, as well as existing routers and VPN concentrators (See *Teknisk forundersøgelse vedr. det internetbaserede sundhedsdatanet*¹(13).

The Internet-based Health Data Net was established at the turn of 2002 to 2003, and, by the beginning of February 2003, the counties (in Denmark) began using the Health Data Net in connection with submitting reports to NIP, the National Indicator Project, at Aarhus County Hospital². Other services such as KPLL (Copenhagen General Practitioners' Laboratory³) and the Health Portal have since come onto the Web.

The Internet-based Health Data Net began actual operation in August 2003, and the pilot project was brought to a close at a meeting of the Infrastructure Work Group under the MedCom Internet Strategy on 2 October 2003.

0.0 Aim

The aim of the Health Data Net is stated in

¹ *Preliminary technical study re the Internet-based Health Data Net*

² Århus Amtssygehus

³ Københavns Praktiserende Lægers Laboratorium

- MedComs Internet strategi⁴, HBJ/CDP/LHF; 29 June 2001 (10)
- Fremtidens sundhedskommunikation⁵, MedCom; December 2001 (11)
- MedCom IV Status, planer og projekter⁶; October 2003 (12)

The aim of MedCom Internet Strategy is to make it possible spontaneously

- to communicate securely on the Internet with users on other "secure" connections
- to utilize all the communication possibilities Internet technology provides.

These aims necessitate establishment of "secure access" between existing "secure networks", and simple rules and regulations for all stakeholders who participate.

0.0 Stakeholders

The Health Data Net will be used for communication between all parties of the health sector. To be connected, a stakeholder must apply for formal approval from MedCom.

Following formal approval and in cooperation with the Health Data Net operations manager, the stakeholder can establish the necessary VPN connection from the stakeholder's net to the Health Data Net node. However, a VPN connection cannot be used until bilateral agreements have been reached with other stakeholders who are connected to the Health Data Net. The bilateral agreements determine who may speak with whom and with which protocols at the IP level.

⁴ MedCom Internet Strategy

⁵ Health sector communication in future

⁶ MedCom IV Status, plans and projects

2 The Health Data Net

2.1 Status on beginning operations in August 2003

On beginning operations in August 2003, the status of the Health Data Net was as follows:

- Web searches (in operation)
- SFTP transfer of data (in operation)
- Edi-mail (developed and currently being tested, though not in operation)
- Video (developed and tested)
- Web mail (currently being tested)

2.2 Subscribers to the Health Data Net in August 2003

The Health Data Net has initially established connections between “secure” data nets in all counties in Denmark, the Municipality of Copenhagen, Copenhagen Hospital Corporation, the Ministry of the Interior and the Ministry of Health, as well as two suppliers of medical systems.

The pharmacy net has been connected and edi-mail exchange has been tested, although it has not been put into operation.

Service providers connected to the net include NIP, KPLL, the Health Portal, and the SUP base (Standardized Retrieval of Patient Data) in Vejle County.

3 Technical solution

3.1 The technical solution

The Health Data Net consists of a central node through which all traffic between stakeholders is routed. Thus, to be connected to the Health Data Net, stakeholders must establish a VPN connection from their own “secure” nets to the Health Data Net node. There are rules and regulations for connecting to the Health Data Net. See *Sundhedsdatanettet: Anvendelse, sikkerhed og ansvar* (3) and “Best practice” ved opkobling til Sundhedsdatanettet⁷ (17)

An illustration of the Health Data Net is included at the end of this report.

3.2 VPN, GRE, IPSec, Internet connection, Agreement system, Summaries and operation status, Security

VPN

Traffic at the central node of the Health Data Net, is routed by a Cisco router. Establishing a VPN connection to the central node takes place between external addresses, which can be accessed on the Internet. Subsequently, the only internal Health Data Net addresses, which can be accessed, are those for which there is a two-party agreement. However, there is an exemption, as the test server on the Health Data Net may be accessed without an agreement. The Internet address of the test server is: <http://www-test.uni-c.medcom>, and the IP address is: 195.80.242.2. See *Tilslutning til sundhedsdatanettet*.⁸ (2)

As differences may occur in VPN standards, it can in some cases be necessary for VPN connections to be established between equipment from the same manufacturer.

⁷ *The Health Data Net: use, security and responsibility* (3) and *Best practice in connecting to the Health Data Net*

⁸ *Connecting to the Health Data Net*

As the supporting medium for VPN connections, the intention is to use the existing Internet connections, which all individual stakeholders currently have.

GRE and IPSec

A very important security function in the Health Data Net is the access control between the individual systems of the institutions, which are connected to the Net, which is performed by a central unit in the node. The precondition is that each connection is treated as a virtual interface in the central unit, so that the individual connection can have filter rules attached to it which, with current technology, is best done with a GRE tunnel.

The data must be encrypted, for which IPSec is used. In other words, it is necessary to have a GRE tunnel encapsulated inside an IPSec connection. 3DES encryption is used.

Internet connection

It would be natural to make a number of requirements to stakeholders' Internet connections, which are used as supporting mediums in the Internet-based Health Data Net. These requirements will include:

- operation stability
- communication speed
- monitoring

The specific requirements will depend on the individual stakeholders, as well as the services to which they subscribe. For example, a 512 Kbit/s connection would presumably be over-dimensioned for a GP, whereas a 2 Mbit/s connection would be too small for a county.

To begin with it appears, that all stakeholders, which have been connected until now, have been able to fulfil the requirements, which the Health Data Net might reasonably be expected to make.

Agreement system

A Web-based agreement system has been developed, enabling the data provider (service) and the data user (client) to indicate which service (IP address) may be accessed by which clients (IP addresses) and by which protocols (port numbers).

After an agreement has been concluded in the Web-based agreement system, it is forwarded electronically to both the data provider and the data user for signature before the connection is opened.

A new stakeholder is registered in the UNI•C agreement system and is assigned a small net (number of connected Health Data Net IP addresses). After this, it is up to the local administrator to register agreements in the agreement system, which can be accessed on the open Internet at <https://aftale.medcom.dk>. See *Agreement system for the Health Data Net*. (4) and (5)

Summaries and operation status

Nodes are monitored, by pinging the central router from a test server. A curve of response times is displayed on the home page of the agreement system at <https://aftale.medcom.dk>.

Here, users can also read important messages on the operation status of the Health Data Net.

Local administrators can distribute operation status messages by sending emails to the mailing list: drift-status@sdn.uni-c.dk. See *Maillister*⁹ (10).

There is also response time accumulation for both ends of the individual VPN channels. The summaries can be accessed only by technicians, and only on the Health Data Net.

Security

The Health Data Net is a private net, which operates at official addresses that are not routed outside the Health Data Net, and which therefore cannot be accessed from the outside. Moreover, a zone transfer from DNS requires special permission. Maximum precautions have thus been taken to prevent hackers from reaching the central DNS server or the net in general, as well as from obtaining information on the nature and design of the net.

3.3 IP addresses

The Health Data Net uses its own IP addresses. For use by the Health Data Net, the UNI•C has been assigned a /20 net, 195.80.240.0 - 195.80.255.255 by RIPE

⁹ *Mailing lists*

(Réseaux IP Européens). When this assigned block of addresses has been used, the UNI•C, as operator, will request a new block of addresses from RIPE.

Like the first addresses, the new IP addresses will be registered as “Provider Independent” and will, according to an email from RIPE dated 10 March 2003, be transferable to a new LIR (Local Internet Registry). In the event of a new provider taking over operation of the Health Data Net, UNI•C will release the IP addresses, which have been registered for the Health Data Net, provided RIPE approves.

The IP addresses of the Health Data Net can only be used in the Health Data Net, i.e. there is NAT (Network Address Translation) between the IP addresses of the Health Data Net and the local addresses. Static NAT is used for services on the net. Port and Address Translation (PAT) is used for clients to the greatest possible extent. On several nets, IP addresses are assigned dynamically by DHCP. If traceability to individual machines is desired, DHCP servers must be enabled to record a relevant/useable log of the addresses assigned.

3.4 DNS

A new local Top Level Domain .medcom has been established (the name was chosen arbitrarily). This new Top Level Domain can only be accessed within the Health Data Net, as it does not exist on any DNS server outside the Health Data Net, which is an internal net with IP addresses, which are known only within the Health Data Net (/20 net, 195.80.240.0 - 195.80.255.255).

All DNS enquiries must be forwarded to a DNS cache, either directly to the Health Data Net node or to a local cache which is configured to forward Health Data Net enquiries to the central DNS caches, i.e. enquiries regarding .medcom as well as 240-255.80.195.in-addr.arpa.

There is a DNS database for .medcom at the central node. In addition, there is a DNS cache which can answer recursive enquiries for .medcom. Both machines are doubled to achieve better redundancy.

As the Health Data Net is a closed net, the Health Data Net cache cannot search information on Internet addresses outside the Health Data Net.

To enable this, DNS caches must be configured locally to handle the top domain .medcom, which is possible with nearly all types of DNS caches. If any related problems should arise, the operations organization of the Health Data net will help find a solution.

Zone transfer from the central DNS server should not be necessary. All data in the MedCom DNS database can be transferred with a zone transfer from the DNS server. Using zone transfer requires special permission.

3.5 edi-mail

Mail server

The MedCom Infrastructure Working Group has determined that ordinary email between persons may not use the .medcom ending. However, email using the .medcom ending may be used to send structured messages between systems on the Health Data Net, including EDIFACT messages encapsulated as email, which are known as edi-mail. Therefore, in the following text, “mail server” refers only to a unit which processes this type of email.

The MedCom Infrastructure Work Group has also determined that there should not be only one mail server, but that all providers of services (VANS providers) should be able to place a mail server on the Health Data Net. A mail server on the Health Data Net must be approved by MedCom, and it must fulfil the norms stipulated by MedCom with regard to security, operations, collection of statistics, etc. In practice, the type of mail server, which a VANS provider will place on the Health Data Net, is a Smart Host. See the definitions below, as well as *Driftskrav til Smart Hosts*¹⁰ (7).

- Smart Host: A Smart Host is a special type of mail server, which relays mail to other smart hosts or mail exchangers on the Health Data Net, and collects statistics etc. In future, the mail servers of the Health Data Net at VANS providers will be known as Smart Hosts.
- Mail Exchanger: A mail exchanger is a mail server, which receives mail on the Health Data Net on behalf of one or more domains.

Edi-mail format

EDI letters are sent via the Internet by means of the MIME 822 standard (email), which specifies how an EDIFACT message is to be attached to an email.

An EDIFACT message is thus the same as using VANS, with the exception that edi-mail aims to send only one UNH letter in each EDIFACT envelope. The VANS providers KMD Net and DanNet convert to and from their own in-house format, to the MIME format.

¹⁰ *Operation requirements for Smart Hosts*

As security against character conversion during transmission, the attached EDI-FACT message must be converted to Base 64.

Addressing

Like the existing EDIFACT communication, location numbers are used for unequivocal indication of sender and addressee. All senders and all addressees must be listed in the Partnership Table of the National Board of Health.

Addressing is done by filling in the MIME sections “To” and “From” with the respective addresses of the addressee:

edimail@lokationsnummer.medcom

and the sender:

edimail@lokationsnummer.medcom

”Edi-mail” currently appears automatically for addressee and sender in the user ID section of all EDI mail.

Routing

The central DNS will contain an MX record for each domain (location number .medcom). Here, Smart Host can ascertain which other Smart Host edi-mail should be sent.

Each system (location number) is associated with one – and only one – Smart Host. The provider (Smart Host) of the system is registered in the Partnership Table.

See *Den gode edi-mail*¹¹ (6)

3.6 Video

The Internet-based Health Data Net can be used for videoconferences, but it is necessary to be able to transport the H.323 protocol to avoid (Network Address Translation). In other words, videoconferences require a special set up which is described in *Medcom løsningsforslag til videokonference hos Vejle Amt*¹² (8).

¹¹ *The good edi-mail*

¹² *MedCom proposal for videoconference in Vejle County*

3.7 Web-mail

Work is in progress to provide a PICNIC Collaboration IT service for Web mail. PICNIC is a mutual EU project for development of secure and user-friendly health data nets. See the description of the PICNIC project on the MedCom home page under “International Projects”.

4 References

- 1 Router configuration (printed on request)
- 2 Tilslutning til sundhedsdatanettet¹³, LS, UNI•C; 13 August 2003
- 3 Sundhedsdatanettet: Anvendelse, sikkerhed og ansvar¹⁴, MBE and IBL, version 1.2, UNI•C; June 2003
- 4 Agreement system for the Health Data Net, KMO and IBL, version 1.0, UNI•C; December 2003
- 5 Dokumentation af Medcom projektets aftalesystem. Systemdokumentation for aftalesystemet med tilhørende scripts for overførsel af ACL lister og indsættelse af (lokationsnumre) MX-records i DNS, KMO, UNI•C¹⁵; 19 December 2003
- 6 Den gode EDI-mail¹⁶, MBE and IBL, version 1.2, UNI•C; 27 January 2003
- 7 Driftskrav til Smart Hosts¹⁷, MBE and IBL, UNI•C; 24 January 2003
- 8 MedCom løsningsforslag til videokonference hos Vejle Amt¹⁸, Lars Hillerup
- 9 Maillister¹⁹ (based on standard system), records of existing mail lists, LS, UNI•C; December 2003

Background materials:

- 10 MedComs Internet strategi²⁰, HBJ/CDP/LHF, 29 June 2001
- 11 Fremtidens sundhedskommunikation²¹, MedCom; December 2001

¹³ Connecting to the Health Data Net

¹⁴ The Health Data Net: use, security and responsibility

¹⁵ Documentation of the agreement system of the MedCom project. System documentation for the agreement system, with the scripts for transfer of ACL lists and entry of (location numbers) MX records in DNS, KMO, and UNI•C

¹⁶ The good edi-mail

¹⁷ Operation requirements for Smart Hosts

¹⁸ MedCom proposal for videoconference in Vejle County

¹⁹ Mailing lists

²⁰ MedCom Internet Strategy

²¹ Health sector communication in future

-
- 12 MedCom IV Status, planer og projekter²², October 2003
 - 13 Teknisk forundersøgelse vedr. det internetbaserede sundhedsdatanet²³, MBE and IBL, version 1.1 , UNI•C; April 2002
 - 14 Sikkerhed i lægepraksis, Praktisk vejledning²⁴, MBE and IBL, version 1.0, UNI•C; October 2002
 - 15 The Danish Health Data Net: Application, Security and Responsibility, MBE and IBL, version 1.2, UNI•C; June 2003
 - 16 H.323 Videokonference i Sundhedsdatanettet²⁵, Dan Mønster, UNI•C
 - 17 Notat "Best practice" ved opkobling til Sundhedsdatanettet²⁶, Fyns Amt, Økonomi- og Serviceafdelingen, IT-Kontoret, Planlægningssektionen, Peder Illum Hansen; 24 April 2003

²² MedCom IV status, plans and projects

²³ Technical preliminary study re. the Internet-based Health Data Net

²⁴ IT security for GPs, a practical guide

²⁵ H.323 videoconference in the Health Data Net

²⁶ Best practice in connecting to the Health Data Net

5 Illustration of the Health Data Net

