NKS/EKO-4.2(96)1 November 25 1996

Nordic System for Data and Information Exchange

Report from meetings with the authorities, and proposal for further work

Tord Walderhaug, Geislavarnir ríkisins

Summary

The EKO-4.2 project involves investigating approaches to setting up a new reliable system based on computer internet technology for exchange of information between the Nordic countries. According to the project plans this information exchange is to be based on bulletin board systems in the different countries. It was required that the system should not set any restriction of type of data or information to be exchanged, nor should it involve any standardization of data, and above all, it was not intended as an alert system. A bulletin board system is passive in the sense that no information is actually sent, instead it is the receiver who is responsible for approaching the information and transferring it to own system. This feature makes the system unsuitable for alert purposes.

Since a potential system will have to be implemented by the authorities in the respective countries, the first part of the project was to survey their interest and emphasis. This was done in meetings in the different countries. The conclusion from those meetings was an overall interest in establishing a system as described, and several requirements concerning security and reliability of the system were proposed. The implication of the requirements by the authorities is discussed and a practical solution of an information exchange system based on the World Wide Web (WWW), the File Transfer Protocol (FTP), and the Internet is outlined.

The continuation of the project must be based on operable servers in the different countries, whose configuration and connection with the local network are the responsibility of the institution owning the server. The selected system will depend on hardware and on the overall security policy of the institution involved. It is proposed that further work concentrates on a general testing of the system, standardizing of server user interfaces and testing of encryption software for transfer of passwords.

Content:

1. Introduction

The purpose of the EKO-4.2 project is to study how information exchange between the Nordic countries, which today is based mainly on telefax, can be transformed to a system which uses computer internet technology. The system proposed in the project plan had the following characteristics:

- Not intended as an alert system
- No restrictions on the data or format of the data to be exchanged
- Should be operated as a Bulletin Board System, i. e. information is only made available, while the actually transfer is performed by the receiver of the information.

The project was initially formulated as a two-step process. First the authorities should express their needs and expectations of an information exchange system, and then this information should be used as a base for setting up a system.

The first part was solved with meetings between the person responsible for the NKS EKO-4.2, Tord Walderhaug, and the respective authorities: Hannele Aaltonen and Heikki Lemmelä at STUK (FI) September 21 1994, Christer Viktorsson and Kjell Nyholm at SSI (SE) December 1 1994, Jens Hovgaard at Beredskabsstyrelsen (DK) August 3 1995, Finn Ugletveit, Tore Ramsöy and Torsten Jütte at Strålevernet (NO) August 10 1995, Sigurður M. Magnússon, Sigurður Emil Pálsson and Þorsteinn V. Jónsson at Geislavarnir (IS) October 4 1995. In addition a combined mini seminar and work meeting with participants from all the countries was held in Reykjavík December 8 and 9 1995. At the work meeting experts on computer networking delivered lectures on security issues in connection with the Internet and on encryption as a method for implementing data confidentiality, and the representatives from the different countries discussed the continuation of the project.

The following persons are EKO-4.2 contact persons in the different countries: Jens Hovgaard, Beredskabsstyrelsen, Heikki Lemmelä, STUK, Tord Walderhaug, Geislavarnir, Torsten Jütte, Strålevernet, and Kjell Nyholm, SSI.

In the following the main goal of the project is clarified and the main topics discussed at the meetings with the authorities are presented. A proposal for a test system and the continuation of the project is presented in the last paragraphs.

This report, together with the protocols from the meetings with the authorities, the agenda and some of the notes from the work meeting in Reykjavík, are available at http://www.geirik.is/eko-42/. More information on how to approach this information is given in paragraph 4 below.

2. About information exchange between Nordic authorities and the EKO-4.2 project

2.1 Current information exchange procedures

The following scheme is currently in use for exchange of information between Nordic emergency authorities in case of nuclear accidents:

1. Alerts are send by telefax to different contact points in the Nordic countries.

2. Additional messages and information are sent to the different authorities either by telefax or by e-mail messages.

3. A Bulletin Board System approach, based on the Internet, has been set up for the exchange of gamma monitoring data.

As can be seen, the telefax has a key position in the information exchange system. Its main advantage is reliability. It is based on the telephone network which has a very high priority by the telephone companies, and is in addition easy to maintain. If a fax machine should e.g. break down, a new one can be plugged in without any complicated set up procedures. Its list of drawbacks, on the other hand, is extensive. The most important being:

- Poor image quality of the messages which can lead to reading errors
- The information can not be processed further without being entered again

This initiated the EKO-4.2 project to investigate approaches to setting up a new system for exchange of information using computer internet technology.

2.2 Types of information to be exchanged

The information to be exchanged between Nordic authorities in case of nuclear accidents can be classified into two types:

1. Alerts and notifications which require an immediate distribution. The originator of the message is responsible for sending the message.

2. Other information not expected to be of immediate importance for the receiver. Examples are further clarification and description of the situation including graphical presentations such as contamination maps and weather maps.

Computer internetworking built on current technology and communication lines would hardly conform to the requirements normally attributed an alert system, the most important being:

- Very high reliability
- Communication failures must be detected quickly, so other channels can be used

Even though a computer network is build upon the telphone network infrastructure, giving it first priority with regard to communication lines, it will not render the same reliability as the telefax, since the computers themselves, with their complicated configurations are more vulnerable to system failures than a fax machine, and much more difficult to replace in case of a failure. The procedure of announcing communication failures is also inferiour to the telefax. The telefax is based on point to point communication, i.e. a physical connection is opened between sender and receiver which is held open as long as transfer of data is taken place, and any failure is easily detected and reported immidiately to the sender of the information. An alert system based on electronic mail will work differently. When a mail is send, the application delivers the mail to a storage area, and from there a background process proceeds by trying to deliver the mail, using the appropriate network protocol. If a network connection fails, and the mail is not delivered, the mail message is normally not returned immidiately to sender, instead the process will terminate. The background process then sweeps periodically through the mail storage area for undelivered mails and tries to retransmit them. It is not until an extended time has passed (can be hours or even days), before the process returns the mail to the sender with an error message.

An alert system based on electronic mail would on the other hand have several favourable characteristics lacking in a system based on the telefax. Most important is the possibility of configuring the receiving computer to automatically give a notification of an incoming alert message. It is therefore without doubt the future solution.

With the above in mind it was realised, already when the EKO-4.2 project plan was formulated, that the project should only address the information exchange described under point two above.

2.3 Mailing list versus bulletin board systems

Information exchange with internet technology can basically be set up in two ways, either as an electronic mailing list, or as a bulletin board system. The former method lacks an automatic acknowledgement procedure. This is not important for short messages, but is a problem in transfer of bigger files. The receiver is on the other hand notified of the existence of new information. The bulletin board system does not need any acknowledgement procedure, since it is the receiver who performs the actual information transfer. This approach, however, has no

automatic notification of new information available for transfer, and may need to be complimented by electronic mails about the content of the servers. The EKO-4.2 project has concentrated on information exchange based on bulletin board systems in each country. It is expected that this approach will make the information exchange more effective, since only information reckoned interesting is transferred, and it may imply a decrease in the use of other communication lines, such as telefax and telephone.

2.4 Dedicated internet versus domestic internet based system

Allthough it is possible to base the system on a closed internet using leased or direct dial-up telephone lines or high performance lines, it has not been considered in the project. Such a solution would above all be very expensive, but also difficult to organize and maintain. The favourable characteristic with regard to security is also deceptive. A truly closed internet is as difficult to intercept as the telephone system (which is very secure, at least in the Nordic countries). The security, however, depends on the system continuing to be closed. If only one of the parties decides also to communicate with another network, e.g. the Internet, the security may be breached. It has therefore seemed more appropriate to discuss a system based on the Internet, identify the security problems and come up with acceptable solutions to them.

The actual establishment of an information server is the task of the respective authorities. The selected system will depend on the hardware, network architecture and degree of security required by the institution. The EKO-4.2 project on the other hand can address specific problems related to the implementation of a system. Examples which have been proposed at the meetings with the authorities are security issues when configuring local net for communication, e.g. different firewall solutions, specification of requirements for the security of data server and data, study of encryption methods and transfer of passwords, or specification of a directory tree for a discretionary access control. In addition the EKO-4.2 contact persons will be able to collaborate on problems encountered when actually configuring a server for the defined purpose, and test the system afterwards.

3. Summary of the discussions with the authorities and at the work meeting in Reykjavík

The discussions were based on an information exchange model outlined in the EKO-4.2 project plan, where each of the involved parties operates a data/information server, which can be reached by the others either over a global computer network (the Internet) or by direct dial up connection.

The development of the system can be based on the Internet, with the possibility of transferring

it to another computer network later. All the authorities were interested in establishing a system as described, and the following requirements were proposed:

- Security of the local network must not be comprimised.
- Security of the information and the information server host computer must be ensured
- Confidentiality of information must be ensured
- System must allow access restriction with discretionary access control
- System must be highly available and reliable
- System must be easy to use

3.1 Security of local network and information server.

The greatest concern of the authorities when operating an information server as described above was related to security of their local network and information server host computer. As mentioned in the previous paragraph, the owner of the local network is solely responsible for the communication, and the configuration will depend on the institution's own network security policy. The NKS/EKO-4.2 project cannot interfere in the dispositions of the different authorities. Beneath are some general remarks on configurations of local network and information server for communication with other networks.

The security of a computer network engaged in communication with other networks, depends mainly on how the network is configured for the communication. Several options are available, from the information server being completely isolated from the local network, i.e. the data must be transferred to and from the server by means of diskettes or some kind of dial-up connection (a 100% secure solution), through different configurations with the local network involving specially configured gateway computers (firewalls) that check, route, and label all information passing through them, see figure 1 - 3. In the first configuration the local network is actually not engaged in the communication at all, instead the information server operates as a network in its own right.

The information server (the host computer) cannot be 100% protected. Firewalls can increase the security, but even then break-ins can be expected. They will however be rare (every few years), brief (the firewall system is quick to detect anomalies), and inexpensive (serious incidence involving system damage and data loss is very unlikely). The system must, however, be used with the risk in mind, and confidentiality of information through encryption must be considered.

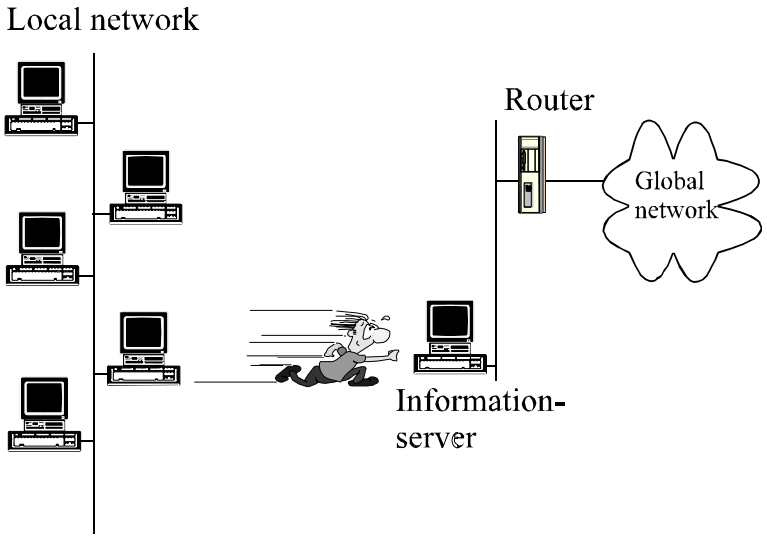

Figure 1. No connection between local network and information server. Data is passed between the local network and server with diskettes.

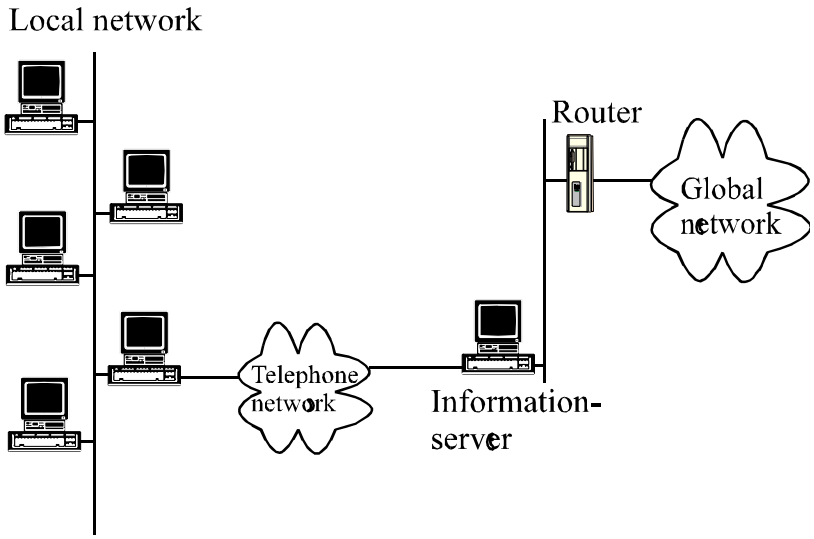

Figure 2. Direct dial-up connection between the local network and information server. By configuring the dial-up connection correctly, 100% security for the local network is available. The extra connection to the server on the other hand, may decrease the security of that part of the system.

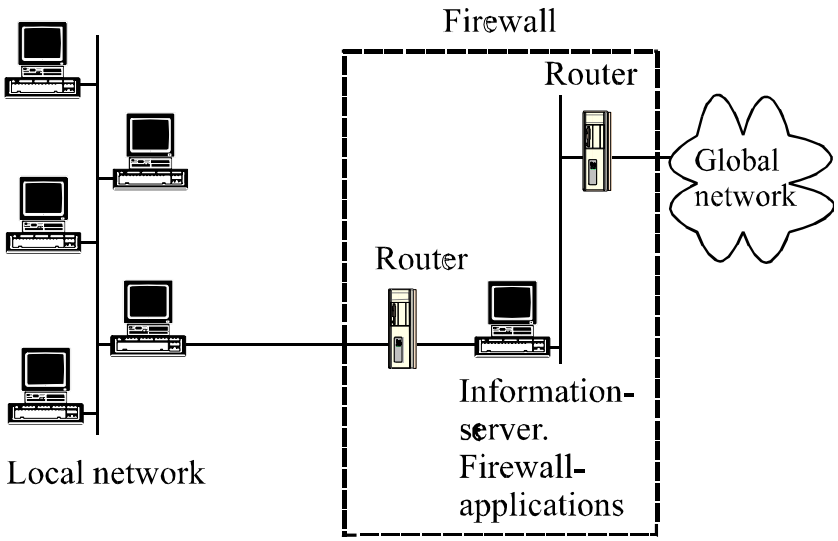

Figure 3. Configuration with a firewall. The local network is not 100% protected. However, it is very unlikely that break-ins will have serious consequences.

3.2 Access restriction

Confidentiality and integrity of the data was also emphasized at the meetings with the authorities. Encryption is a straightforward way to ensure both. Access restriction must apply, and even a discretionary access control is of interest. Different kinds of access restriction can be achieved through the use of user identification procedures when attaching the data server, or the data server or its router to the Internet can be configured to deny requests from all but some specific networks (packet filtering).

3.3 Encryption

At the work meeting in Reykjavík, encryption of data was especially discussed, and a lecture dealt with the PGP encryption routine.

While the local network can always be satisfactorily protected, the data itself, through break-ins in the information server or interception in transfer, can never be secured. Encryption of the data can solve this problem. It is interesting to note that an increased information exchange is now going through the electronic mail system between the authorities. Those plain language messages may easily be intercepted in transfer. The institutions have in addition often based their mail system on external providers, without knowledge of security measures established on those servers.

Messages encrypted with the newest methods (e.g. the RSA or IDEA algorithm) are practically unbreakable. In addition, the problem of a secure distribution of encryption keys can be solved with public key cryptography. It involves both a secret key which is kept by the recipient of the messages and used for decryption, and a public key available for all who wants to send messages to the recipient and is used for the encryption. Thus, anyone can encrypt messages intended for the recipient, but only the recipient can decrypt them.

If encryption on a daily basis is going to work, it has to be done automatically. For electronic mail, it is expected that the software developers will attach the possibility to their software (and some systems already have the possibility), while for an information server as described in the EKO-4.2 project, a routine which automatically encrypt all messages made available on the server has to be developed. Public key cryptography must be used for exchange of encryption keys for those messages.

3.4 Availability of information system and data

The Internet has not the same availability as the telephone network, since many telegraph companies, give leased lines for computer networks second priority with regard to availability. A reserve line, e.g. direct dial-up connection, is therefore necessary as a future solution. However, in the meanwhile the telefax may also be regarded as a reserve system. It is important to note that software used on the Internet, also can be employed on direct dial-up connections. The connection can therefore be moved from the Internet to an ordinary telephone line without the user noticing any change.

3.5 Accessibility

It was stressed at the meetings with the authorities that the system must be easy to use. Fortunately, software developed recently, most notably the server and browser software for the World Wide Web (WWW), has made information exchange with TCP/IP and the Internet very user friendly.

The software for transferring files to the system, i.e from local network to the server, must also be easy to use. This software is, however, dependent on the local network technology and operative system, and how the data server is configured with respect to the local network, and will therefore differ between the countries. Several commercial and free software packets for "drag and drop" copying of files between the local network and an external internet server, are available.

3.6 Other topics discussed at the meetings

The different countries have presented their local network topology together with plans for connection to the Internet. Different possibilities of establishing a server have also been discussed. It may for instance be possible to operate the server from another organization, institutional or private. A close collaboration with the system manager at the external organisation is then needed, since some of the setup implicate changes to the system configuration which only system managers have access to.

Several other projects exist which include data communication between computer networks has been identified. Most notably is the exchange of gamma monitoring data between the Nordic countries, which is based on TCP/IP. Norway has also planned to use TCP/IP as a part of their decision making tool system in case of a nuclear emergency, and Sweden is going to implement a network based on UUCP between SSI and the different local authorities hosting a nuclear power station.

The possibility of identifying a set of requirements to use as a base when developing a system have been discussed. Such requirements could involve security of the data made available on the servers, availability of the servers and, requirements regarding the speed and flexibility of the network. At the moment, however, it is not regarded necessary.

Some countries may be interested to present additional information intended for the public on the same server. The implication of such a configuration on the availability of the server has been discussed. In case of a nuclear accident a rush on the server of the public seeking information may be expected, and this may affect the availability of the server. A general increase in traffic on the Internet could also be expected in case of a major nuclear accident, which may affect the overall performance of the Internet and thereby the information exchange system. A backup system based on other physical links is therefore necessary to ensure reliability.

Different operative systems have different rules regarding allowed length and type of characters in the filenames. It is therefore convenient to agree upon a standard form of the filename and extension of the files made available on the servers. A classical DOS filename format (8.3) should work on all systems.

4. Description of a test system

An example data server which closely matches the requirements specified in the previous paragraph has been set up at Geislavarnir ríkisins. It is based on CERN httpd World Wide Web server software running on a Unix computer with a firewall connection to local network. The

transfer of data is accomplished with the File Transfer Protocol. The server can be found at `http://www.geirik.is/eko-42/`.

The server presents three directories with different information. The “Test directory” consists of different kind of data files which can be downloaded by a mouse click. The directory listing is automatically updated when new files are made available. This directory can be used to test features of the information exchange, such as encryption. The next directory presents monitoring data from the Reykjavík gamma monitoring station. This directory is automatically updated once every 24 hours. It can also be reached directly with the File Transfer Protocol for automatic downloading procedures. The last directory contains a WWW version of this report and some additional information about the EKO-4.2 project. All the directories require user identification to access the information. The user name and password for the test directory and the directory with a WWW version of this report is:

- Test directory: User name: `test`
  Password: `carpe4d`

- EKO-4.2 reports: User name: `info`
  Password: `eko.News`

For those without access to the Internet, figures 4 - 6 show how a session where a file is down loaded may appear, using Netscape Navigator browser software to access the server. On figure 7 is shown how a new file is made available on the server.

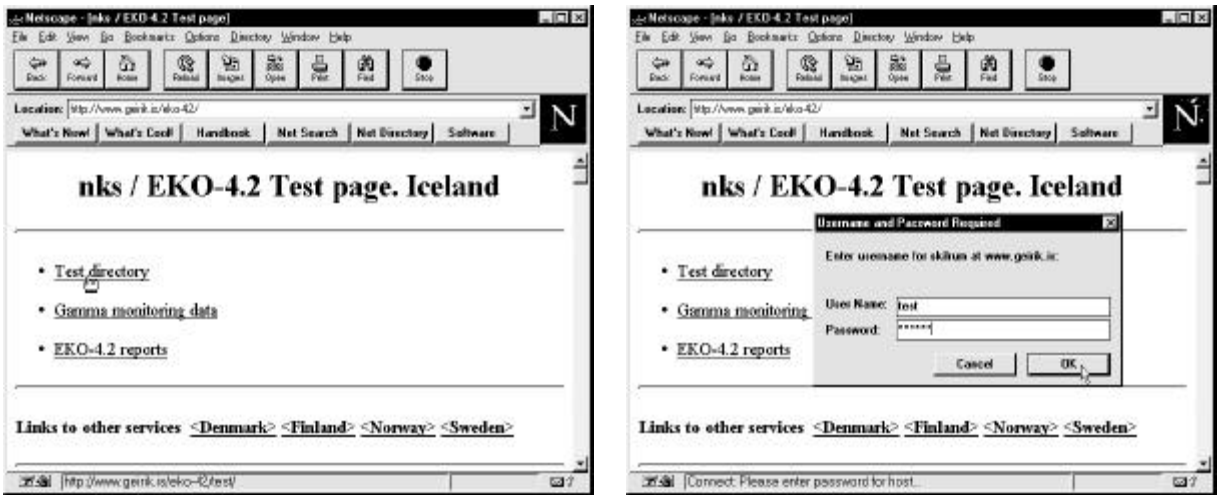

Figure 4. A user interface of an information server showing different directories containing data, as well as links to similar services in the other Nordic countries (left). The directories are password protected with different passwords for discretionary access control. When a directory is selected, a window pops up acquiring user identification (right).

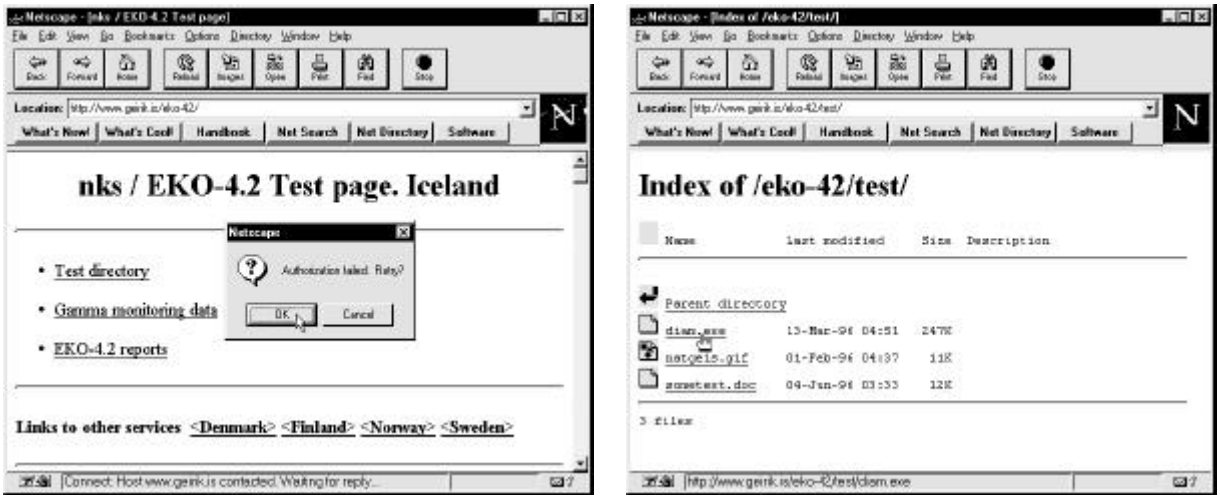

Figure 5. Incorrect user name or password is notified with an "Authorization failed" message (left), while a correct user identification gives access to the directory with the information (right). The different files can now be transferred to own system with a mouse click.

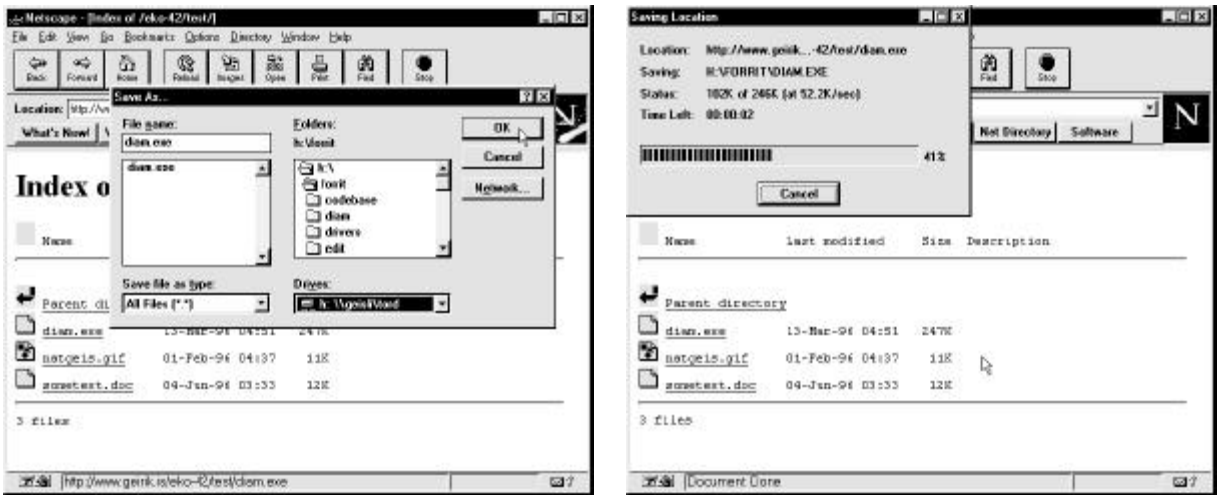

Figure 6. When a file is selected, the user is first asked where to save the file on own system (left), and the file is then transferred (right).

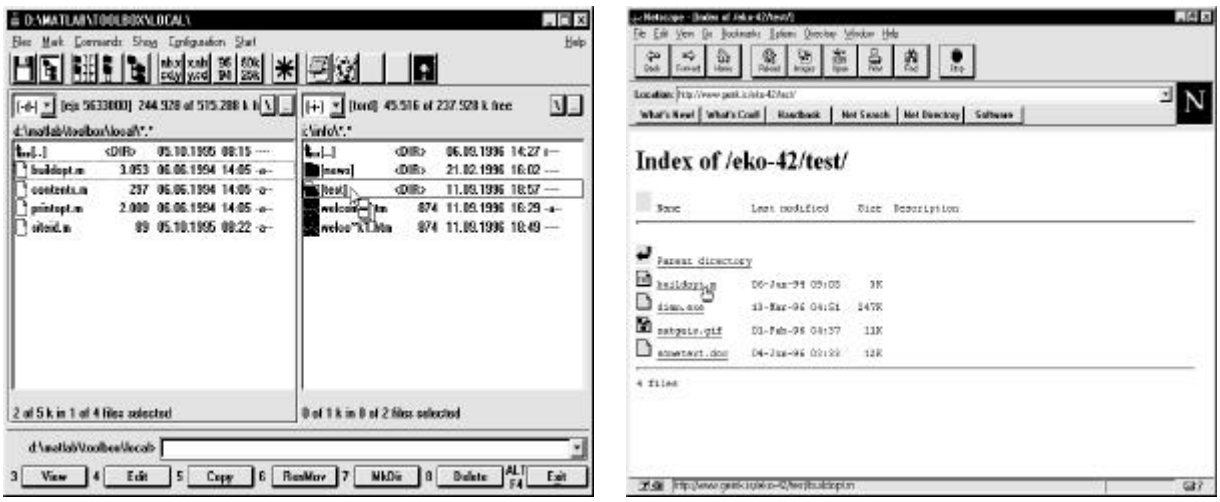

Figure 7. A new file is made available on the server. The server is set up as a drive on the computer network, and files can be copied across the firewall with a standard file manager (left). The directory listing is automatically updated and the remote user has now the possibility of approaching the new information (right).

5. The continuation of the project

It is important to note that the example in previous paragraph is far from the only way, and probably not the most convenient way of exchanging information. Different approaches are needed for different purposes. It may for instance be of interest to automatically transfer data of a certain kind, and then a solution with a direct use of the File Transfer Protocol must be applied instead of going through the World Wide Web. The current development in the field of telecommunication is very rapid, and better information exchange solutions will certainly be introduced in the future. An example is remote access to computer systems, which today is regarded as highly insecure, but which in the future may be an interesting alternative.

Further work must be based on operable servers in the different countries. It requires that every country both set up a server according to own criteria and security requirements, and develops tools for approaching the information in the other countries. Proposed topics of interest to study further in addition to an overall testing of the system, are:

- secure transfer of passwords
- encryption, including automatic encryption routines
- standardisation of user interfaces and directory tree for discretionary access control

All further work must be in close cooperation with the involved authorities.