Interviews carried through

Appendix 1

XXX responsible for the current system.

Date 2002-03-15
Place X
Time 10:00 – 10:45

XX at the security department for X
Date 2002-03-10
Place X
Time 10:00 – 10:45

Anders Renefjord Regionmanager WM Data

Date 2002-04-12
Place WM Data Karlskrona
Time 10:00 – 11:00

Göran Bergström Accounting Manager at company Y

Date 2002-03-12
Place Phone Interview

Ann-Christin Nilsson FöreningsSparbanken/Ljungby.
Date 2002-03-12
Place Phone Interview

Bertil Nordlöf Strålfors
Date 2002-03-25
Place E-mail interview

Peter Bievesand Security Consultant
Date 2002-05-21
Place E-mail interview

Daniel Pettersson Security Consultant
Date 2002-05-09
Place E-mail interview

Ulf Jonsson IT-Consultant at Invia
Date 2002-05-13
Place E-mail interview

Interview with Göran Bergström at Y

1. Does Y provide its customers with an electronic invoice system today?

Yes, we offer our private customers to precede their payment process through their bank's home site. A service offered through cooperation between Föreningssparbanken and Nordbanken.

2. Will you provide your business clients to pay with the same system in the future?

Answer: Yes, we are planning to let them pay electronically too.

3. What kind of solution does Y use to transfer the files to the bank?

Answer: WM Data has built the technical solutions.

Question to FöreningsSparbanken

Appendix 3

How big are the customers using the bank over Internet and what criteria must be fulfilled?

A company that is using the bank over Internet is containing between 0 and 50 employees. They have to fulfil four different criteria to be able to use this service and the four criteria are size, engagement, transactions or employees.
This service is used for different things smaller companies are using it to get information and to pay their invoices. Bigger companies are using it for getting information about accounts and so forth.

Ann-Christin Nilsson FöreningsSparbanken/Ljungby

Interview with XX at X

Appendix 4

1.What kind of network does X use?

Answer: Locally a LAN and between other offices a WAN.

2.What kind of transmission rate does the 32-channel ISDN connection to Strålfors provides?

Answer: Each channel provides 63Kbt. The connection uses as many channels as necessary due to the line's current traffic.

3. Does X have a security policy?

Answer: Yes, and it will be available for you but within restrictions for publishing.

4. What is your response to file transfer by mail as with the Current system?

Answer: It is acceptable to e-mail an invoice according to our security policy but the human interaction regarding the encryption function may be a security risk.

5. Is the fact that the sender at X has to start the encryption session by him/her self a security risk?

Answer: This is the main issue and problem when it comes to sending the file by mail.

6. What is the most severe threat from the Internet?

Answer: Viruses are the largest threat from the Internet. If the customer considers the information on the Invoice as very sensitive the fact that a company's secret information leaks out is a risk.

7. To protect information over the Internet, what kind of security does X provide?

Answer: Firewalls and antivirus programs, though the latest virus will always come through anyway.

8. Transferring a file with ISDN provides safety copies at both X and Strålfors, while the Invoice is copied two times within the same physical building, how does these facts effect the security aspect?

Answer: If X use the ISDN connection there will automatically be two copies one at X and another at Strålfors which of course is good, but the back up security at X is safe enough. Back up is taken continuously and the tapes are places in a special "firesafe" cell. The tapes are then within short intervals transported to a safe place at another physical location. It is also a fact that two many safety copies from the moment the file is created until it is send may lead to loss of information.

9. What kinds of threats are possible from outside regarding the ISDN connection?

Answer: In order to establish connection with Strålfors, X sends a signal with a code to Strålfors, which performs a check up with its router, where a password to break the code is stored. If someone wants to cut the connection they have to go through Telia' s switch and then in to the router to steal the password. The probability of someone to try all this to only to get information from invoices is very low, almost non existing.

10. What kind of security weaknesses do you see in the current system?

Answer: The human interaction and the number of safety copies.

11. Is the ISDN connection secure for sending the invoice file?

Answer: Very safe.

12. We have thought about the possibility to use a mail server for the storage and encryption of the files, from where the file automatically could be transferred to the customer, what is your reaction to this system?

Answer: It is good but you have to find an encryption program, which encrypts automatically.

13. Do you know any safety consultant that X use and we could ask some questions?

Answer. Yes I will take contact with Peter Bivesand for you.

14. What communication protocol is used in the ISDN channel?
Answer: Today we are using RCP.

15. Do you think that the file needs to be encrypted before being sent over the ISDN channel?
Answer: I do not think that the file needs to be encrypted as long as a password or checksum or similar is used.

16. Do you think that Stallings Security Services are important and needed to fulfil the company X's security policy.
Answer: Yes, I think that this is required for X. I think that all these security services are important especially within the transmission of an invoice over a communication network.

Interview with Anders Ranefjord region manager at Wm-Data Appendix 5

Which services does Wm-Data provide?

Wm-Data is offering everything from the installation of one computer to an entire network and different system constructions like: billing, payments and other systems.

Is there an increased trend towards billing via Internet banks?

I cannot see this trend, but I think it will increase. What I do see is that electronic billing or to be exact electronic transfer of information is increasing. I do not have any evidence of this it is my professional perception.

Which security threats do you see?

- Hackers
- Viruses, new ones always arise.
- The biggest threat is from within the organisation. I can see how important the security issue has become for the companies. This has increased enormously the last three years. Many organisations are inquiring risk analyses and handbooks in security.

How much of system development is security?

80% of the system development is security thinking and this is not something that even was considered 20 years ago. Today a system has to be security qualified at the start of the development.

How do you consider an acknowledgement should function?

It is very important to be assured that the information send is the information received. An example is: how many rows, the amount of letters every row consists of and how many A's etc. that the document contains.

Which risks do there exist with e-mail?

E-mail is the most risky system. Most things go wrong with e-mail. For example: the mail does not arrive, it can be altered, virus can be send and the addresses are not hard to come across. The employee's unawareness results in that they open their mails without concerning the risks and in that way the employee becomes a security risk. Here it is important with well-established security policies. E-mail is the easiest way to sabotage and create huge damage.

Which provides the user with most security, ISDN or a fixed channel?

I think that ISDN is more secure because the time you are connected is limited. And the probability of someone hacking at that time is very small. With a fixed channel you are permanently connected and therefore more vulnerable.

Which profits can you see with electronic commerce?

It will provide you with a smaller stock, and less consumption of paper.

Interview with Daniel Pettersson, secode Appendix 6

1. **In a security perspective, which advantages and disadvantages do you consider there exist with our ISDN solution?**
2. **In a security perspective, which advantages and disadvantages do you consider there exist with our X.25 solution?**

   These solutions use ISDN or X.25 instead of TCP/IP. The choice of protocol on link level does not affect the security since so called "end-to-end" security must be achieved to secure the transmission. End-to-end security means that a transmission from one application (sender server) to another (receiver server) must be secured in the top level in the OSI-model. For example: Several banks use for example encryption/authentication on link level between routers. This guarantees that the router really are who the say they are and that no one can bug the traffic between them. But this measure does not secure a FTP transaction that passes these routers. In the protocol layers above there still exist all former vulnerabilities. Link encryption is used in this case only as an extra measure.

   An advantage with using ISDN or X.25 is that these media are not so well known. This does on the other hand not provide functions that makes them extra secure, but since these are less known there exists fewer attackers with knowledge about how they can be used. If a protocol like TCP/IP is used there suddenly exists a very large group of people that are "experts" on this protocol and can thus use its weaknesses. If TCP/IP also is used over a public network such as Internet the risks are of course increasing.

3. **In a security perspective, which advantages and disadvantages do you consider there exist with our mail server solution?**

   File transferring can be done by the help of a number of protocols. Mail (SMTP) as mentioned in this solution is an alternative, even though this protocol in it self (without extra RFC extensions) does not provide any authentication. The problem with securing access to the private key does not arise for the transmitter, unless you receive encrypted information and wants to decrypt it automatically. But the same problem arises when a file is signed, since a signature is necessary to guarantee that the file transmitted to the receiver can be verified afterwards. This is a necessity for secure transactions, that the identity of the executor of the transaction (signature) can be verified. Note that signing is needed for verifying the integrity of the transaction. Anybody can otherwise take the receivers public key, encrypt a file and send it to the receiver.

4. **Do you consider it to be a necessity that business information that is sent between two parties, should contain identification and verification?**

   Yes, when it comes to business information it should afterwards be possible to trace who has made a transaction and also be able to prove with a digital signature that the transaction is acknowledged by the receiver. "Non-repudiation" is very important when it comes to transactions. An orderer should not after be able to state that he/she did not order a product. Likewise shall the seller's electronic "receipt" be used by the orderer to prove that he/she has paid the product, even if the seller states differently.

5. **What do you consider to be the most secure file transfer?**

   A secure implementation of signatures and encryption of the invoice files presents good security level at transactions. This together with well protected private keys and with for example SSH as transfer protocol where RSA/DSA keys are used for identification of users. The private RSA/DSA keys can then be stored on smart cards to reach an additional level of security.

Peter Bivesand at Calineb

Appendix 7

What advantages and disadvantages do you think that the mail server solution have when it comes to security issues?

Answer:
Advantage: Very cost effective. It is easy to install and today every body use e-mail.

Disadvantage: The e-mail must be encrypted and decrypted. If this is done on Internet connected systems the security level is decreased. If it is done on systems that are not connected to Internet and it is only the encrypted file that is moved out to the Internet is it much more secure.

Ulf Jonsson IT-consult at Invia

Appendix 8

1. Does there exist any kind of identification and verification of a packet received in an X.25 network?

Answer: Yes, there exist an in built function that make sure that all packets must be received with the right checksum otherwise resend the packets until everything is OK, otherwise an error message is sent. All nodes that are involved are reporting back that everything has gone OK.

2. Is it possible for someone from the outside or the inside to tap the traffic and if so is it then possible to understand the data as it is composed of ones and zeros?

Answer: Yes unfortunately can that happen, but it is very difficult for anyone to know which way an X.25 packet will take as it do not need to take the same way every time. This depends on loading, problems with the wire or nodes and so on.

One other thing is the function called Closed User Group (CUG). This means that the operator create a group of the X.25 numbers that the company use and it makes it difficult for others to get in from the outside. It is also called FAP-net.

3. Is it possible for an X.25 network to be infected of a virus and if so can the virus come from the out side or is it only possible from the inside?

Answer: As I see it the threat must come from the inside. There are too many controls to be able to attack from the outside but today can no one be sure about this either.

Strålfors

Appendix 9

The company was founded 1919 in Ljungby Sweden and started in the printing business. Today it is an IT-focused organisation operating in 11 countries. Strålfors is working in the area of information transfer and is a supplier of overall solutions for e-commerce, card solutions paper based information and IT solutions etc. Since 1964 Strålfors has moved its operations globally and co-operate with its headquarters abroad.

The company's goal is to serve businesses in order for them to focus on their own core operations. By intense research for the development of technical solutions Strålfors wants to optimise its customers need. Strålfors is currently expanding in Scandinavia with its closure of two agreements with Oberthur Card Systems (leader within smart-card solutions) and Dmdata (leader within information management and IT operation).

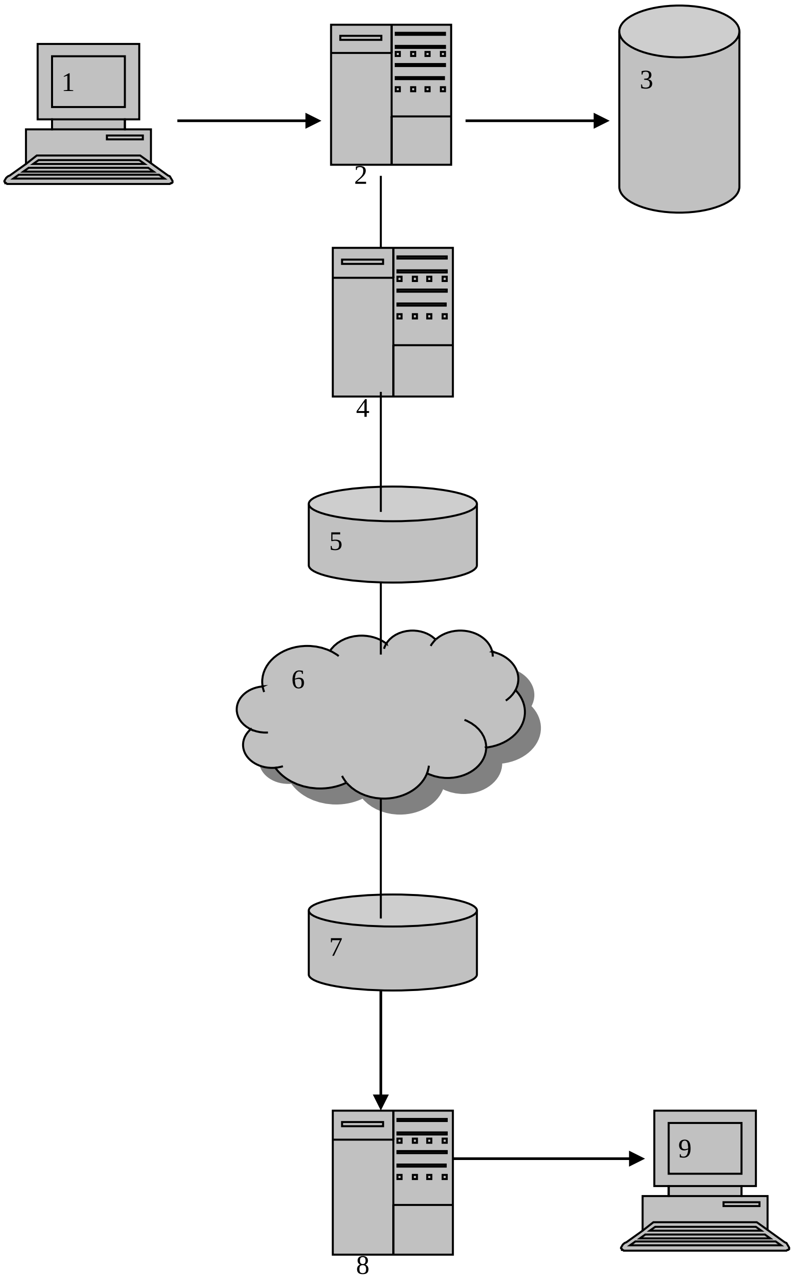
Strålfors now offers two new concepts to its customers called Minterbase and Information Logistics. These concepts are based on services like

- Credit card-processing
- Database management
- Printing and security solutions
- Logistics
- Electronic postal system
- Data convention for both paper-based and electronic flow

The new company, StrålforsInformation Logistics A/S, has estimated net sales of MDKK 130 for the year 2002.

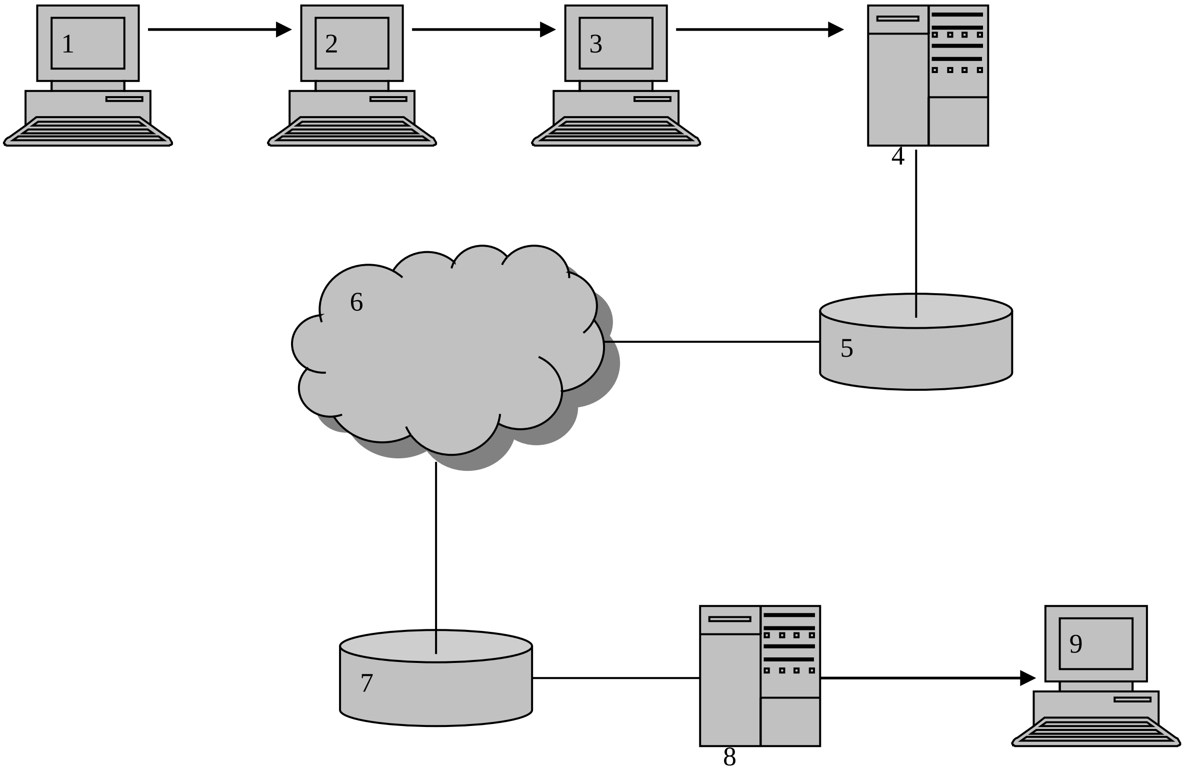
Mail server

Appendix 10



1. **X client:** In this level the file is formatted into the final appearance of the invoice. Before it is sent to the encryption server the invoice is copied to another file on the client.
2. **X encryption server:** The invoice is placed in the encryption server and automatically encrypted.
3. **X database:** The mail server is connected to a database where the customers' addresses are stored.
4. **X mail server:** The invoice is placed in the mail server and an e-mail to the customer is developed and automatically send.
5. **X firewall:** The invoice package is forwarded through the firewall.
6. **Internet:**
7. **Customer firewall:**
8. **Customer mail server:** This mail server receives the encrypted invoice from X's mail server.
9. **Customer client:** The customers fetch the invoice from their mail server.

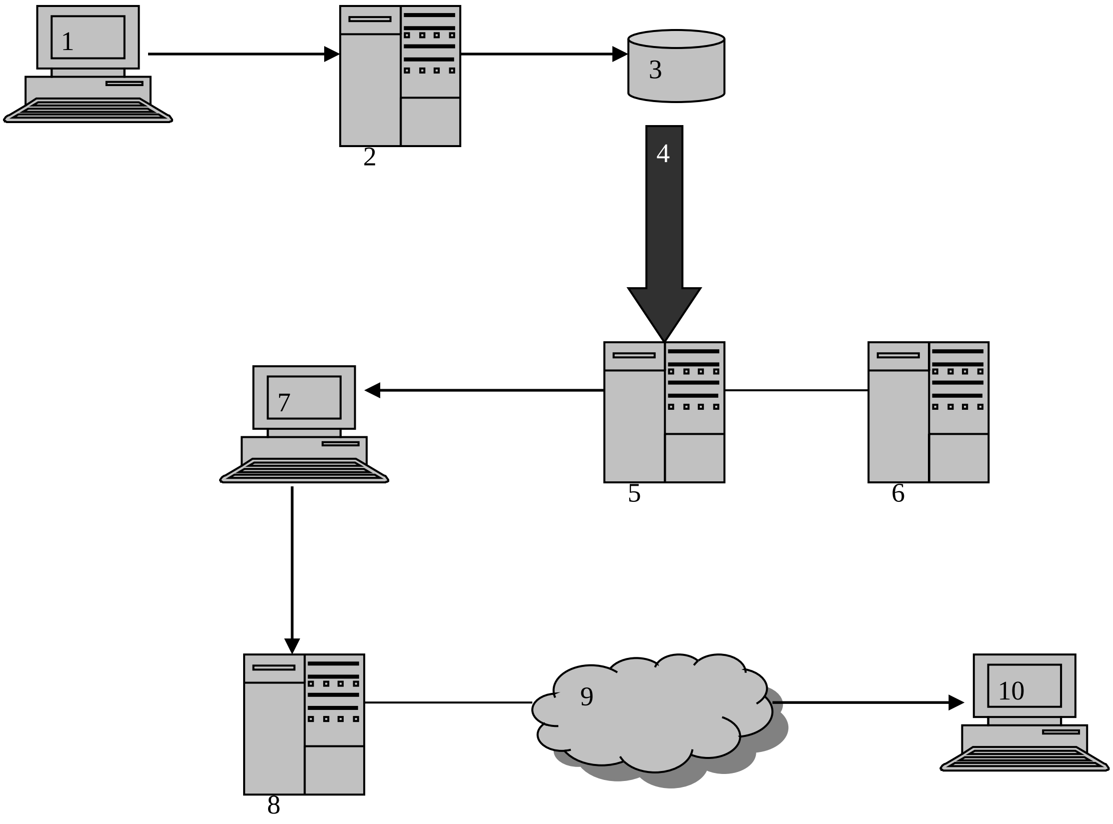
Current system



1. Here all data is collected into a data file, the file is automatically forwarded in seven different periods to level 2.
2. The file is formatted into the final design of the invoice and copied to another file on the server.
3. The mail is compiled and the invoice is manually encrypted and attached before it is mechanically sent to the customer.
4. X mail server
5. X firewall
6. Internet
7. Customer firewall
8. Customer mail server
9. Customer client

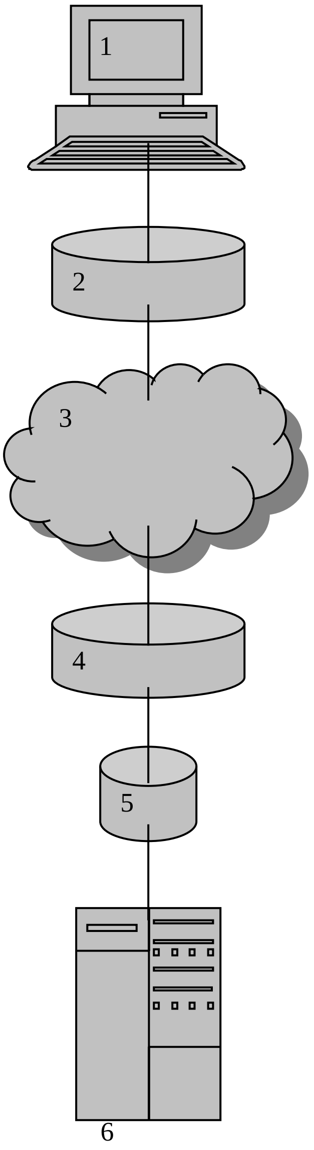
X.25 via Internet bank

Appendix 12



1. X client: Invoice is created and forwarded
2. X's server
3. X's firewall
4. X.25 connection
5. EDI service
6. Webb server: creates the invoice's public format
7. Customer's bank
8. Internet bank
9. Internet
10. Customer client

ISDN via third party



1. X’s FTP client
2. X’s ISDN router
3. ISDN network
4. Third party ISDN router
5. Third party firewall
6. Third party FTP server

Security policy for X Appendix 14

X provides services to customers with high demands for quality and service. A high security level at X is an assumption so that the company can deliver service and services of high quality.

Therefore our goal is that:

- information about our customers do not end up in the hands of unauthorised
- decrease interruptions in our nets and systems that can cause our customers harm or inconvenience
- protect the company's assets
- protect our co-operators mental and physical health
- follow laws and other demands

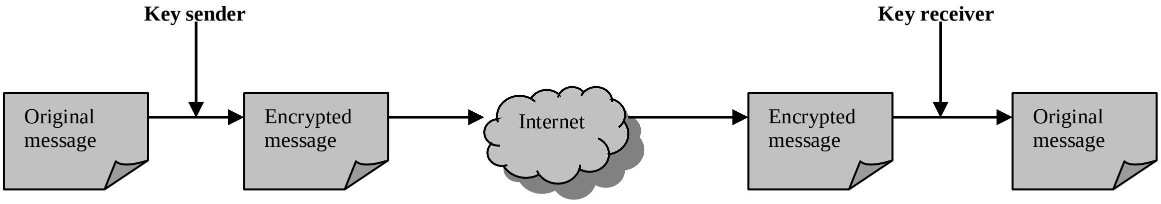
SME Definition Appendix 15
(http://www.tekes.fi/eng/information/sme.html)

Small & Medium Sized Enterprises according to the EU definition

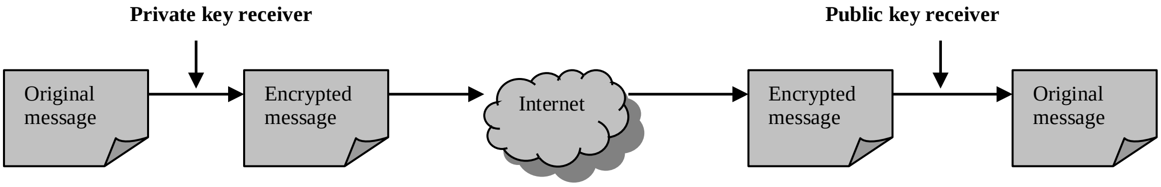
An SME is defined as a company, which:

- employs fewer than 250 people
- has a turnover of less than EUR 40 million per annum or net balance sheet assets of less than EUR 27 million
- must be less than 25 percent owned by a larger company/companies which do not qualify as an SME themselves.

Appendix 16



Symmetrical encryption



Asymmetrical encryption

Picture based on Turbans Secret key cryptography and Public key cryptography.

National Computational Science Alliance

Appendix 17

(http://www.ncsa.uiuc.edu/)

The National Computational Science Alliance is a nationwide partnership of more than 50 academic, government and business organizations working together to prototype an advanced computational infrastructure for the new century. This infrastructure, called the Grid, is rapidly developing into a ubiquitous, pervasive, national-scale information infrastructure that links supercomputers, virtual environments, scientific instruments, large databases and research team.