

Design and Implementation of a Certificate Authority Frontend

Format: conference

Requirements for the presentation: overhead projector or video projector

This paper can also be presented in Spanish

Author information:

Name: Mariana Podestá, Frank Losemann, Thomas Engel, Christoph Meinel

Address: Institut für Telematik, Bahnhofstr 30 –32, 54292 Trier, Germany

Fax number: +49 (0)651-97551-12

Telephone number: +49 (0)651-97551-0

E-mail address: {podesta|losemann|engel|meinel}@ti.fhg.de

Brief resume:

Many enterprises use intranets in order to provide information to their employees only. However, sometimes it is also necessary to restrict access to some of this information. A way to identify who is allowed to use the data and who is not is to issue digital certificates to the users, enabling them to authenticate and authorize themselves for the different intranet resources. The problem is to define an interface for acquiring certificates which is, for one, easily understandable for the users and which, secondly, allows the Certificate Authority (CA) to ensure that the entities requesting the certificates are the ones they claim to be. In this paper, we will describe how we designed and implemented a CA-system solving the problem presented above.

Design and Implementation of a Certificate Authority Frontend

Mariana Podestá
Frank Losemann
Thomas Engel
Christoph Meinel

E-mail: [\[podestallosemann|engel|meinel}@ti.fhg.de](mailto:{podestallosemann|engel|meinel}@ti.fhg.de)

Institut für Telematik, Bahnhofstr 30 –32, 54292 Trier, Germany
Fax number: +49 (0)651-97551-12
Telephone number: +49 (0)651-97551-0

Extended abstract

The number of organizations using intranets has been growing steadily during the last few years. Implementing an intranet results in various advantages such as making use of internet technology and the use of a browser as the intranet's interface. This interface may be widely used for the internet and posses the added advantage that is known by most of the users. Then there is the possibility of employees sharing the company resources without confidential information being made available to anybody outside the organization. However, the problem of determining who is allowed to use certain resources inside the company and who is not still remains. A way to authenticate users to the different resources which the intranet offers lies in the use of certificates. A certificate is a digital document which states that a person is who he or she claims to be.

We have developed a system named „Certificate Authority Frontend“ (CAFE) capable of collecting data information needed for generating certificates for the employees, so that they can use them to authenticate themselves for using the resources of the intranet. For the generation of certificates, we have used a commercially available software-package. Although this software had some templates for implementing the different steps in the process, we decided to build our own interfaces, according to the needs, the usability and the organization of the enterprise.

It is common for people working with computers for an international organization to not be interested in how a program works. It is of no interest to them to know how they have been defined or which properties were used during the design and the implementation of the program. From the point of view of the user it is important to have transparency and an easy-to-handle workflow since he is not interested in technical issues and details. The same is true for the use of certificates. The end-user knows that he needs a certificate although he does not know what it means to acquire one or which properties it possesses . All the user knows is that if he does not have a certificate he will not be able to use some resources presented on the intranet. Thus, what the user needs is a simple “tutorial page“ to get the necessary information and also a user-friendly interface to guide him through the process of obtaining a digital identification. The system should provide easy interfaces with as much information as possible and should let the user acquire the certificate in a short period of time. Also, it has to be developed in such a way that the user has to give some basic information only - such as name and employee number.

CAFE has all the properties described above. Although the system developed here is complex, the process of obtaining a certificate is easy. The user possess enough information for to know what he has to do. He applies for a certificate providing only his name and employee number and obtains a reference. The Certificate Authority (CA) generates a PIN that the user has to deploy later on. He uses the reference and the PIN number to obtain and download his certificate into his browser's database. Users will take advantage of the installed certificate to authenticate themselves for using the resources of the intranet. The details of the whole process are stored and logged in a database which serves, in addition, as a control-tool for the administration of the system.

Our solution differs from other solutions in the following aspects:

1. The whole process for acquiring a certificate is adapted to the needs of an international enterprise, it is not a standard system where the users have to adapt themselves to it.
2. The system guarantees that nobody who lacks the necessary authorization get a certificate in a user's name. This is achieved by using different kinds of protocols during the process.
3. The CA ensures that any particular person who asked for a certificate is who he claims to be. This is done by implementing the „four eyes principle“ for the acceptance of an application. The given data will be checked against the employee-database of the enterprise to verify its validity.
4. A main design goal was to obtain high usability for the user interface, to increase user-acceptance and to lower help-desk inquiries. For a small business of up to about a 100 employees this last aspect will not be all that important but in large intranet environments, it makes sense to improve the certificate-request workflow in even minor details. 6 minutes saved per certificate-request for 10.000 employees means 1000 hours of time saved for working time. By providing a self-explaining workflow, an even greater amount of time can be saved. Working time gets paid for “twice” if users waste time trying to obtain a certificate and administrators waste time explaining the process since neither the user nor the administrator are, during that time, doing what they were hired to do.

CAFE is already in practice, we have begun with 500 users and we are expecting to double this number by the end of the year.

Design and Implementation of a Certificate Authority Frontend

Mariana Podestá
Frank Losemann
Thomas Engel
Christoph Meinel

E-mail: {podestallosemann|engel|meinel}@ti.fhg.de

Institut für Telematik, Bahnhofstr 30 –32, 54292 Trier, Germany
Fax number: +49 (0)651-97551-12
Telephone number: +49 (0)651-97551-0

1. Introduction

Nowadays almost all organizations have an intranet, so that they can have their diverse collection of computing and information resources ready for the use of the employees. These resources may vary from billing systems, library services to employee phone books. But how do these organizations verify the identity of someone, how do they decide whether a certain employee may use a specific resource or not? In situations of accessing network resources, the security issue has to deal with two topics: first, it must be determined whether the user is who he claims to be (authentication), and, secondly, it has to be determined if the specified user is allowed to use the requested resource (authorization).

Authentication is often based on passwords although it is said that this kind of authentication was created for the interaction between humans and computers and not for identifying users across a network of computers [KPS95]. A good solution for this problem is to make use of some kind of cryptographic techniques such as digital certificates in order to determine “who is who”. A digital certificate is a document that confirms the correspondence between an identified individual (owner of a private key) and the public key which is stored in the certificate.

The model presented here was developed for the use in the intranet of a big industrial organization. The main purpose was the definition of a system capable of generating certificates for the employees so that they could use these certificates to get authorized access for the resources of the intranet. For the generation of certificates, we are using a standard software-package. Although this software had some templates for implementing the different steps in the process, we decided to build our own interfaces, according to the needs, the usability and the organization of the enterprise.

First we will explain what is meant by a CA, and what the meaning of the different types of encryption is and how this is connected to the use of digital certificates. Then we will describe the developed model in detail: the most important steps for acquiring a certificate, the role-definition and the security elements implemented to control the process. Finally, we will explain what makes our solution different from that provided by existing commercial solutions.

1.1. Certificate Authority (CA)

A Certificate Authority (CA) is an authority in a network that issues and manages security digital credentials. The CA binds an identity to a public – private key pair. This way somebody intending to communicate with another person simply needs to trust the CA and to accept the certificate of this person.

Trust management following a CA policy can be deployed and interpreted in different meanings. An organization, for example, does not need to trust all CAs in the world. For an enterprise policy within an intranet it is not necessarily important that the issued certificates are accepted by other organizations as they are only used within the intranet. To establish a „world-wide“ trust scenario, different issues like legal codes and the policy of the deployed CAs have to be addressed in the first place. Up to date, these issues are being investigated.

The first action that has to be taken to install a CA is to generate a key pair and to self-sign the public key to create a CA's certificate. This certificate should be published afterwards so that the users can download it onto their browsers. To verify the correspondence between a user and his certificate, the CA signs each certificate with its own private key.

1.2. Kinds of Encryption and Use of Digital Certificates

There are two kinds of encryption: symmetric-key and public-key [MOV97], [Sch96], [Men97]. The symmetric key uses the same secret key to encrypt and decrypt a message. The problem with this kind of encryption lies in the fact that each group of persons intending to communicate with each other need to know this secret key. A better solution regarding the key-distribution problem is the public key cryptography.

The public key encryption uses two keys. Each person has one public and one private key. The public key is given to all the other users so that they can send encrypted messages to the first user. The private key is used by this person to decrypt the messages that he receives. There is also a problem with this kind of encryption, though. What would happen if someone

generated a key-pair in the name of an user and used it to send messages in that user's name? We need a way to make sure that a certain public-key corresponds to a specific person. This can be achieved by using digital certificates.

A digital certificate is a verifiable statement which gives testimony of a correspondence between a person and its public-key (also included in the certificate) [NCS97]. Certificates can not only be used for encrypting messages, they might also be used for authenticating the use of resources on an intranet.

Certificates are based on public-key cryptography. This concept is introduced in [DH76] and was first realized as described in [RSA78]. [Sha49] gives the theoretical background for cryptography.

2. Our Certificate Authority Fronted (CAFE)

We have defined a CA-system to provide the employees of a worldwide enterprise with a simple way to obtain certificates.

There are two kinds of people involved in the process, the end-users and the agents. The end-user is the person who will acquire a certificate. The agents are responsible for verifying all the information that the user provides and also for determining whether the user will receive a certificate or not.

2.1. Certification User Workflow

Goal: Simplifying the process of requesting a certificate for intranet usage, combining available information about users from databases with identifying user's input.

2.1.1. Important steps for acquiring a certificate

Obtaining a certificate is a process that may be divided into three steps. First, as mentioned before, the user has to install the CA-certificate on his browser. This step is important since the installment of the CA-certificate tells the browser that it can "trust" the CA. In the second step, the user has to fill out an application-form (Figure 1) with some basic information such as name and employee-number. As the result of submitting the form he gets a reference-number. If the application is accepted, the user will acquire a secret number (PIN) afterwards.

Third, the user uses the PIN in conjunction with his reference number to obtain and install the certificate on his browser.

This procedure ensures that only the user can download the certificate.

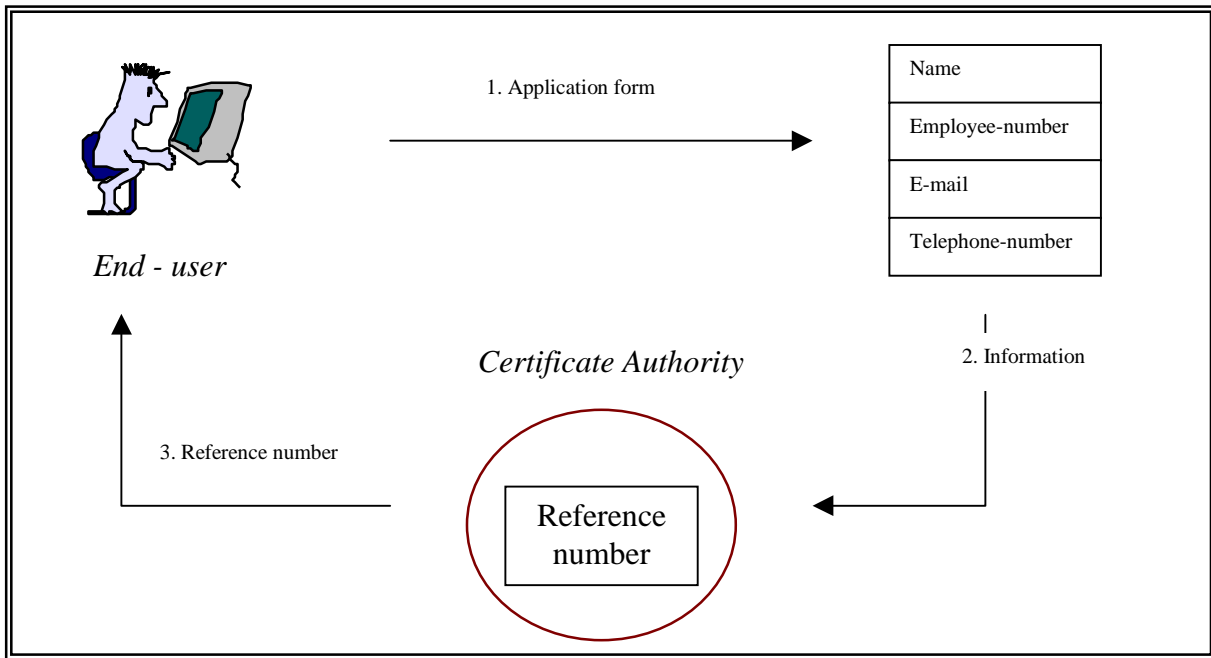


Figure 1: Application for a certificate

2.1.1.1. Installing the CA-certificate

The user possesses an interface containing all the necessary instructions for performing the installation of the CA certificate without any difficulties. The meaning of the dialog-boxes that appear will not be explained to him - he will merely be told how to handle the workflow.

2.1.1.2. Filling in an application form

When the user gives the information to the application form, this will automatically be checked for spelling errors. The errors are corrected comparing the input with the data stored at the enterprise's employee-database. The user then proceeds to a screen where his information is shown (this data is taken from the employee-database, this is the reason why it is sufficient to give the name and the employee number), and he just has to check whether his e-mail address and telephone number taken from the database are correct or not. This is the last interface where the user has to verify his personal data.

The user does not need to care about what happens between his application for a certificate and the time he receives the PIN-letter. If there is an error in the input data of the certificate-

request, it is likely that an agent of the intranet CA will contact him by e-mail or telephone-call. If the application is rejected, the user won't receive a secret number but he will get a letter explaining that the application for the certificate has been rejected.

All the data that is provided by the user is compared with the information stored within the company's database. The CA needs to make sure that the person asking for a certificate really is the same person existing in the company's database.

2.1.1.3. Getting and installing a certificate

To get a certificate, it is necessary to obtain a PIN. A PIN is a randomly generated number sent by mail to each user possessing an accepted application. The PIN is printed in a special format so that is difficult to obtain the PIN without opening the letter.

With this PIN and the number that the user got when he applied for the certificate, he can call the corresponding interface to get his certificate and install it on his browser (Figure 2).

The user has three attempts to obtain his certificate. If he fails three times entering either the reference-number or the PIN, the certificate will be locked. This way, the system prevents people from guessing numbers. To unlock a certificate it is necessary to contact the CA-Administration.

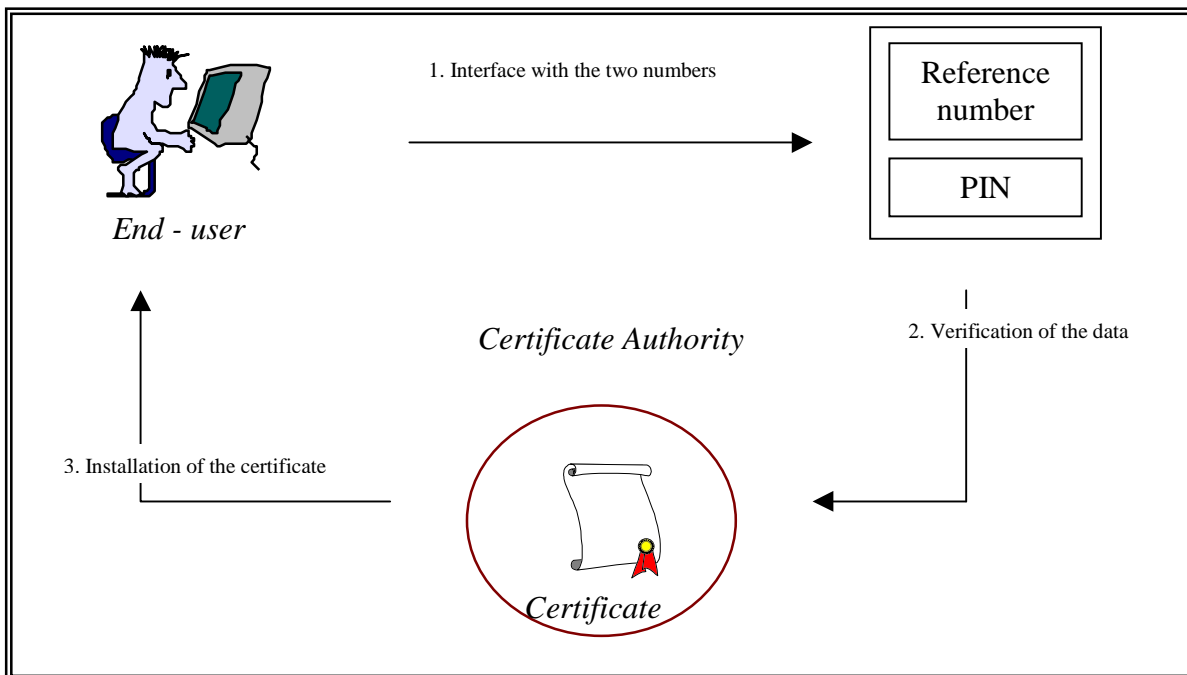


Figure 2: Getting a certificate

2.1.2. Security mechanisms implemented

The information provided by the user can be checked against existing data. In case of a conflict, the CA personal determines whether the databases are outdated or whether the information provided by the user is incorrect.

When the user gets the reference-number at the first interface he also receives an e-mail. This way, a user receiving an email stating that he applied for a certificate when he knows he did not will know instantly that someone is intending to obtain a certificate in his name. At this point the user will be aware that he has to notify the CA-personal so that they can intervene. We also get the IP-Address of the machine where the user applies for the certificate so that we can always find out from which workstation the application originated.

The PIN-letter is printed on a specific kind of form like those used by creditcard companies to send creditcard PINs to clients. The PIN-Letters are sent by mail and the user has to sign on receipt of the letter. In the first place, using this procedure helps the user because, by the condition of the letter, he can determine if it has been tampered with. On the other hand, the CA-personal may determine the whereabouts of the letter if the user has not received it in the specified period of time.

2.2. Certification Agent Workflow

Goal: Ensuring that the entities requesting the certificates are the ones they claim to be by applying checks described in the CAs policies.

2.2.1. Important steps of the process

The process described is completed with the actions taken in the background by the agents of the CA. The main action of the agents is the acceptance of an application. They are also responsible for the printing of the PIN-letters.

2.2.1.1. Acceptance of an application

This might be the most important stage of the system. Here it will be specified which applications are correct so that they might be accepted (Figure 3). The following examinations will be done when receiving an application:

- Is the address on the application form correct? The mail address is needed to send the user a PIN so that he can pick up his certificate from the corresponding interface.

- Do the telephone number and e-mail address given in the application comply with the ones saved in the organization's database? If they are not correct, they have to be verified by making a telephone-call to the user or by sending him an e-mail.
- What is the state of an application? Use of the „four-eyes principle“: when an application is presented to be accepted, it is necessary that the agent is sure that the person who asked for the certificate is who he claims to be. Therefore each application should be accepted by two different agents.

The interfaces developed for the agents have also been developed for easy understanding of the workflow. The state of an application is shown with visual elements (such as pictures) so that the errors of the given data can be detected and corrected immediately. We think it is important that the agent does not lose too much time finding errors in the given data, that it is easier when we show them what is wrong, and that they just have to verify and correct it.

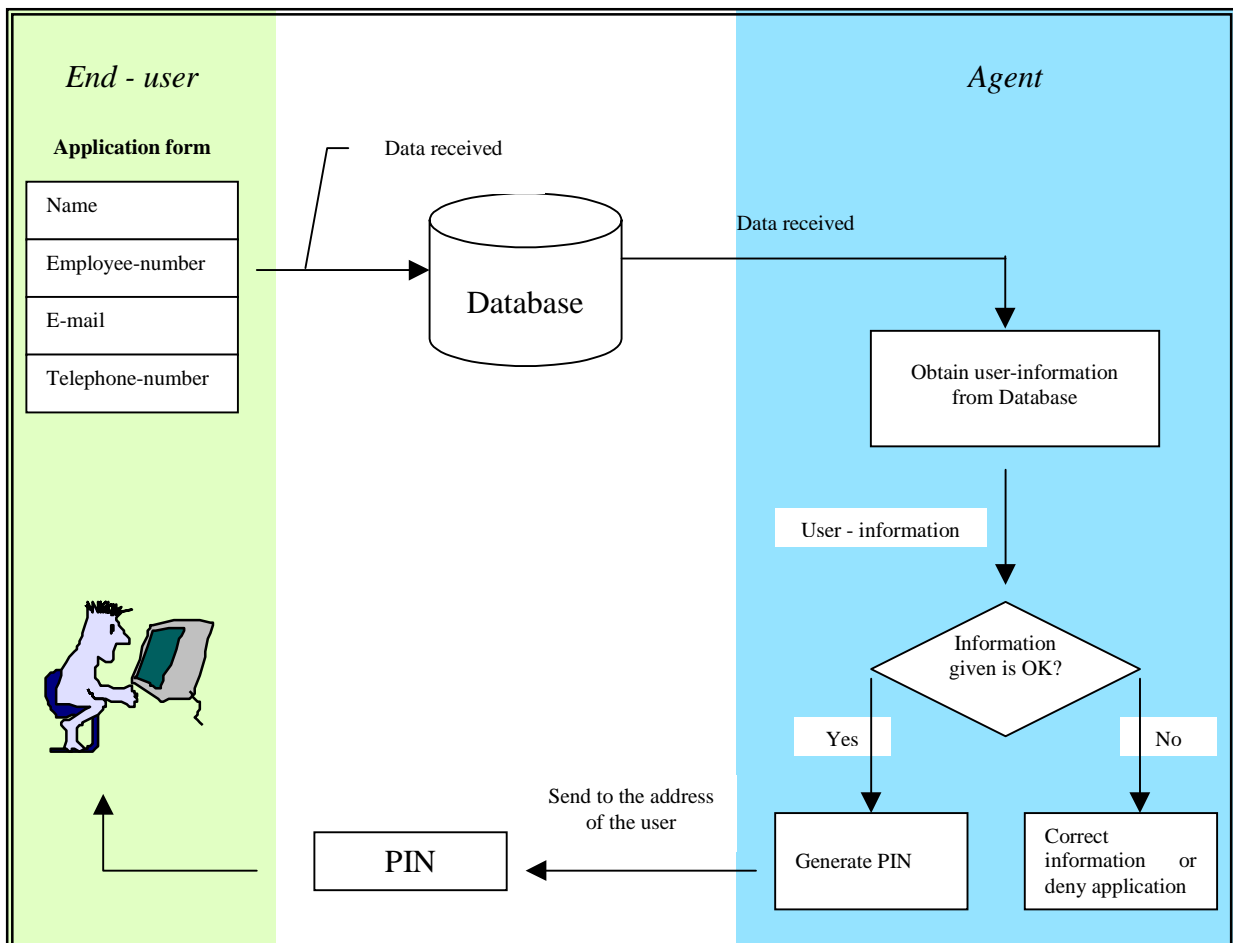


Figure 3: Acceptance of an application

As soon as an application is accepted it is ready to wait for the generation of a PIN.

2.2.1.2. *PIN-letters*

A PIN is a number which is necessary for downloading the certificate. The PIN is sent via mail to each user that applied for a certificate and was accepted by the CA. This number is saved encrypted with a one-way function within a letter-formatted file. This one-way function for encryption ensures that not even the staff of the CA will be able to decrypt it. The generation of the PIN-Letters is made using a batch-job. This letter contains not only the PIN but also the address of the user. As soon as this file is sent to be printed, all the encrypted information will be decrypted directly on the printer. The letters are printed on specific forms and the process is done using the „four eyes principle“ where two agents work together to send the documents to the printer. They also have to fill in a report indicating which files were printed. If there were errors they have to describe them, adding the date and their name. This report is then sent to the CA-Administration. This way, the CA-administration maintains control over the files that get printed and is being kept informed about errors that occurred (if any). Errors occurring during the print-job are usually related to printer problems.

2.2.2. Use of databases

There are two databases included in the system: one is the employee's database where the personal information of each employee is stored. We use this database to obtain the necessary data when the employee applies for a certificate. We also have a database to store all the information necessary for generating the certificates. All the changes that are done within applications get registered with user-name and time when the change was made. We also have defined conditions for the applications. Each application has a specified state while it is being filled out, the state is changing through the different steps of the process until the end of it (i.e. obtaining the certificate).

When an agent accepts an application, all the information that he changes is saved in the database. We have implemented a mechanism to record date, time, action and agent of every action that is being carried out on a request. The information of the agent is taken from his certificate. For this interface, the agent needs to possess a valid, installed certificate. Otherwise the agent will not be able to make any changes on the database. However, sometimes it is possible to have a pair of corresponding username and password for accessing and manipulating the data. Furthermore it is necessary to have a valid certificate so that the authorization for changes in the database will not take place if any part fails.

3. Concluding Remarks

Our main goals for the definition of CAFE were:

1. Simplifying the process of requesting a certificate for intranet usage.
2. Ensuring that the entities requesting a certificate are the ones they claim to be.

We achieved the first goal by defining user-friendly interfaces and presenting a simple way to apply and obtain certificates. The second objective was reached by the implementation of secure protocols, such as the „four-eyes principle“ for checking and approving the applications and other critical tasks. These two objectives are what makes our solution different from a commercial one.

4. References

- [DH76] „New directions in cryptography“
W. Diffie and M. E. Hellman
IEEE Transactions on Information Theory, 1976
- [KPS95] „Network Security: Private Communication in a public world“
C. Kaufman, R. Perlman, M. Speciner
Prentice Hall, 1995
- [Men97] „El ABC de los documentos electrónicos seguros“
I. Mendivil
Seguridata, 1997
- [MOV97] „Handbook of Applied Cryptography“
A. J. Menezes, P. C. van Oorschot, S. A. Vanstone
CRC Press, 1997
- [NCS97] „Netscape Certificate Server v1.0“
Administrator’s Guide for UNIX
Netscape Communications Corp., 1997
- [RSA78] „A method for obtaining digital signatures and public-key cryptosystems“
R. L. Rivest, A. Shamir, and L. Adleman
Communications of the ACM, vol. 21 no. 2, pp. 120-126, 1978
- [Sch96] „Applied Cryptography. Second Edition“
B. Schneier
John Wiley & sons, 1996
- [Sha49] „Communication theory of secrecy systems“
C. E. Shannon
Bell System Technical Journal, vol. 28, pp. 656-715, 1949