



**Institut für Telematik** unter Betreuung der  
Fraunhofer Gesellschaft



**Preprint 2000-12**

**The Necessity of a Public Key  
Infrastructure for a  
Virtual University**

Mariana Podestá  
Christoph Meinel

ISSN 1433-8106



Authors	Mariana Podestá Christoph Meinel
Copyright	© 2000 Institut für Telematik e.V., Trier
Trademarks	Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	12/2000
Document status	Version 1 (30.12.00)
	Printed in Germany All rights reserved
	<p>The documentation was accomplished through the Institut für Telematik. The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the mentioned enterprises must respond to changing market conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication is subject to change.</p> <p>The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.</p>

The concept of virtual university has grown rapidly, in the last few years. The cost of multimedia computers becoming lower and the use of the World Wide Web being more common and cheaper has helped to this evolution.

Many studies have been done about the definition of user friendly interfaces, the presentation of the material by the teachers [1], the need of some kind of human interaction [2], the user support services [3] and of course also about the advantages of life long learning[4].

However, the definition of a virtual university also requires an understanding of not only the different components of distance education but also of the properties that the internet offers [4] and those characteristics which it does not offer, like security and privacy. If we define a way of providing users with security and privacy, then we will be able to create a university, in which the main interaction channel is the web, and where the user needs not to use any other element of communication, such as fax, telephone or mail.

Therefore, we can say that a virtual university is competent, if it can provide the following properties

- *confidentiality*: which provides privacy in the messages using encryption techniques;
- *authentication*: which determines the origin of a message and provides some kind of assurance that it has not been sent by an intruder in the name of the sender;
- *integrity*: which ensures that the message sent is the same as the data received, i. e. the information has not been altered during the communication;
- *non - repudiation*: which means that the sender cannot later deny the authorship of the message sent.

All these properties can be guaranteed by establishing a Public Key Infrastructure (PKI)[5, 6].

### Basic concepts

A PKI is a complex system which uses public key cryptography and digital certificates [7] to achieve security in communications. A PKI is based on public-key cryptography [8]. This kind of cryptography states that each entity in a communication has a pair of keys : a public and a private one. Any data encrypted with a public key can only be decrypted by using the corresponding private key. The public key is publicly available while the private one is only known by the entity to which the pair of keys belongs. To be sure that a certain key pair really belongs to only one person it is necessary to use a specific "document" which binds a public key to one person. Such a document is called a "digital certificate". When a certificate is generated, it is installed in the browser of the user. The private key is stored in a database, which is (normally) located on the user's hard disk. The user must remember only one password: the one that protects his or her database.

## 1 Use of a PKI in a Virtual University

In this section will be described first the elements of a PKI inside a virtual university:

- certificate, directory and timestamp servers, personal security elements and the user components.
- policies
- professionals

and second the use of digital certificates within it in order to obtain the properties described in the introduction. For example

- digital signatures of documents for obtaining the property of non-repudiation
- encryption of data for the needed confidentiality
- timestamp files in order to determine the existence of objects at a particular point of time.

### The Necessity of a Public Key Infrastructure for a Virtual University

Mariana Podestá  
Christoph Meinel

## 1.1 Elements of a Virtual University's PKI

A PKI consists of policies, services and professionals. A policy is a plan of action proposed or adopted by an entity. There are four classes of professionals involved: agents, administrators, designers and end-users. Agents are responsible for the successful interaction between users and services, while administrators are responsible for auditing the services. Each service includes programs for the interaction of users, agents and administrators with the services. These programs are defined by the designers. Finally, we have the end user, who uses every service according to his necessities. He or she interacts with every program defined by the designer and with the servers included in the virtual university. Students, teachers, tutors and administration personal are defined as being end-users.

The components of a PKI for a virtual university will be described in the following five sections.

### 1.1.1 Certificate Service

A Certificate Authority (CA) is the most important component of a PKI because it is the entity that issues, manages and revokes certificates. Through the certificate service, users of an intranet can apply for certificates and obtain and install them in their computers. In the university, net users trust this CA and the generated digital identifications.

### 1.1.2 Directory Server

A directory service is a collection of software which is used to store information about the organization. The goal of this service is to keep university data, so that it can be retrieved later when searching for this information.

In a virtual university the directory server is used to store the data of the users obtaining and using certificates. It is also possible to use several directory servers working in conjunction.

Certificate and directory are two services which may be used together to obtain digital identifications. Normally, people studying at a virtual university do not possess a large degree of computer knowledge. Due to this, the process of applying and obtaining a certificate must be designed to be as simple as possible, with interfaces that are easy to use, thereby allowing the user to need as little information as possible. For example, when applying for a certificate, the user normally has to provide a lot of information about his or her locality, state, country, e-mail, telephone number, etc. Users normally doubt how this information should be specified. According to this, it is better to ask the user for simple information, for example pertaining only to their name and identification number, and acquire all other needed information from the data saved in the directory server. An example of this model could be read at [9].

### 1.1.3 Timestamp Server

A Timestamp Server is necessary in the case of there being a need to determine the existence of a document at a particular point of time.

For example, there are circumstances in which it is necessary that many students take the same examination on the same day, yet at different places. As it is important to ensure the fact that each student has to have the same chances, all examinations should be sent before and after a specific time. In such a situation it is necessary to timestamp each document, meaning that after writing an examination, the student signs it digitally, using his or her valid installed certificate, and then sends it to the Timestamp Server (TS). The TS checks the signature to determine if it really belongs to the student, and, if so, adds a timestamp to it, thereby signing it once again. Afterwards, the TS sends it to the student and to the examination group (EG). Each TS keeps a database with document, user and time. The EG receives the signed document from the TS, verifies the signature and obtains the examination of the student with the corresponding timestamp.

This server can be used in order to[10]:

- have a trustworthy time server in an IP-net
- include the date and time in a digital stamp bound to any digital object
- produce a digital timestamp for any valid document sent by any valid client

#### 1.1.4 Personal Security Elements

Smart cards, diskettes and even hard disks can be used as personal security elements for storing private keys.

#### 1.1.5 User Components

User components describe the different elements and resources that are available at the university for the user, like chats, newsgroups, e-mail programs and learning material. The tools necessary for applying, acquiring and using certificates are also part of this section.

### 1.2 Use of Certificates

In the following, we will explain the different uses that certificates have within a virtual university.

#### 1.2.1 Authentication

When logging into a virtual university, the user normally has to provide his or her username and password (basic authentication). It is possible that for specific resources a password may also be required. This is a problem for the user, who is forced to remember different passwords. From the security point of view, we know that all information sent over a TCP/IP network passes through various computers until its destination is reached. An eavesdropper may see, change or alter the data being sent. Basic authentication may serve as a good example for such an attack, passwords (if not encrypted) are sent in clear over the network. Therefore, we propose the use of a single sign-on solution (SSO) based on certificates (strong authentication) and on the Secure Socket Layer (SSL) protocol. This solution consists of a one time authentication to the server, which thereby permits access to all the resources without any additional passwords. The strong authentication is based on the fact that the user has a certificate and on the fact that the user knows the password that protects his or her private key. Although in this kind of authentication a password is also needed (to gain access to the private key database), this does not indicate a possible danger because the password is not sent over the network. The private key is normally stored in the local computer.

Users in a virtual university are divided into groups, such as students, teachers, tutors and university administration. Subgroups are also included in order to distinguish, for example, between students of different careers and/or different semesters. The Access Control Lists (ACLs) are used to determine which group has access to which resource and if authentication is needed and, if so, to request for it. Using the installed certificate of the user, the server will be able to determine the user's identity and by using the directory server ascertain the group and whether or not the access may be accepted.

To conclude, the following are clear advantages to this kind of authentication:

- users have only to remember one password
- passwords are not sent over the network, avoiding security risks
- installed certificates enable users access to the virtual university and all its resources

#### 1.2.2 Digital Signatures

The use of digital signatures helps to prove the origin of data (authentication), verify whether the data has been altered (integrity) and determine whether or not the apparent sender is also the actual sender of the data (non-repudiation).

Digital signatures can be used to determine:

- authorship of resources, exercises, books
- sender of e-mails
- applications for information
- subscription to newsgroups
- identify documents within the university administration

The procedure for signing consists of giving the password that protects the private key's database and in using the private key to encrypt the data. The receiver decrypts the data using the public key of the sender and in this way verifies the sender's signature.

### 1.2.3 Encryption of Data

Encryption provides confidentiality within communications, that is to say privacy in the messages and data. It is valuable for the following procedures:

- sending credit card numbers for paying the university tuition
- sending personal / private information to the university administration
- using e-mail
- obtaining the results of exercises and examinations confidentially
- distributing research results
- authorizing personal data of students only to specific people
- notifying specific people of private events

In order to encrypt data using certificates, the sender uses the public key (stored in the certificate) of the receiver. Encryption can also be combined with digital signatures in order to obtain its properties.

### 1.2.4 Timestamping Files

Timestamping can be used when doing partial examinations on-line, in situations in which the teacher states the time of begin of an examination, and makes the exercises available to all the students. In this situation all students must have the same chances: they all receive the examination at the same time, they have the same amount of hours to finish them. Results sent after the deadline are not to be considered. Timestamping can also be used successfully for the following situations:

- application to the university administration
- enrolment in courses with a limited number of students

## 2 Conclusion

In this preprint, we have presented the different components of a PKI integrated into a virtual university. We have also proposed the use of digital certificates for encrypting and signing information, for authenticating documents used by and within the virtual university and its resources and for timestamping documents and files. The benefits of the use of PKI inside a virtual university are clear. Now, it needs only to be studied how the interfaces for obtaining certificates and using them will be defined, enabling users a trouble-free period of adaptation to this new tool.

## References

- [1] L. Carswell: *The 'Virtual University': Toward an Internet paradigm?*, 6<sup>th</sup> Annual Conference on the Teaching of Computing, Dublin, Ireland, 1998
- [2] D. Casey: *Learning "From" or "Through" the Web: Models of Web Based Education*, 6<sup>th</sup> Annual Conference on the Teaching of Computing, Dublin, Ireland, 1998
- [3] R. J. Tucker and J. Cordani, *Teaching Teachers to Teach On-line*, ACM's Special Interest Group on University and College Computing Services (SIGUCCS), 1998
- [4] A. Eurelings, et al., Hg., *Integrating Information & Communication Technology in Higher Education*, Kluwer - Deventer, Masstricht, 1999,. Gastkemper, F; pp. 181 – 192
- [5] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1996
- [6] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. , *Handbook of Applied Cryptography*, CRC Press, Florida, 1997
- [7] M. Hastenteufel, C. Meinel, *Digitale Zertifikate – Standards und Anwendungen*, Institut für Telematik, Technische Berichte, 99-01, 1999
- [8] W. Diffie and M.E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory , 1976
- [9] M. Podestá, F. Losemann, T. Engel und C. Meinel, *Design and Implementation of a Certificate Authority Front-End*, DISC, México, 1999
- [10] J. Dávila Muro, L. Fincias, *Diseño y realización de un Servicio de Sellado Digital de Tiempo*, CriptoLab – Facultad de Informática – Universidad Politécnica de Madrid, November 1998