# 11 THE PRODNET COMMUNICATION INFRASTRUCTURE

A. Luís Osório*, Carlos Antunes, Manuel M. Barata
ESTEC, Estudos e Tecnologias da Informação, Portugal

*The electronic information exchange between enterprises requires the deployment of an infrastructure able to cope with all the associated complexities. Communication availability, quality of the communication services, information security, compliance with the governmental legislation, are only some of the complexities emerging from such required communication infrastructure. This chapter presents the PRODNET communication infrastructure as a proposal to deal with those mentioned constraints, giving the enterprises a secure mean to electronically exchange their business documents.*

## INTRODUCTION

This chapter aims to present the PRODNET communication infrastructure preceded by a definition of a basic survey on communication technologies. Some of the included aspects are:

- the emergence of a group of *de facto* standards most of them associated to the Internet paradigm with a significant acceptance by the main computer industrialists;
- the need for third parties playing the role of mediators between traders and governmental institutions as the right security/legal framework to support the business-to-business electronic commerce;
- different facets of cryptographic technology to protect and authenticate sensitive commercial information;
- the integrating perspective of the PRODNET communication infrastructure by the inclusion of different communication resources offering extended flexibility.

The last developments in computing and communications lead to a panoply of technological solutions, most of them converging to cover similar requirements creating, however, an heterogeneous space, difficult to contribute to a uniform and

* ESTEC Lda., TAGUSPARK, Edificios Tecnologias I, N. 21, 2780 Oeiras, Portugal,
Tel: +351-1-4220120, Fax: +351-1-4214090, lo@estec.pt

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35577-1_37

L. M. Camarinha-Matos et al. (eds.), *Infrastructures for Virtual Enterprises*

cooperative system. Based on the requirements established for the PRODNET II virtual enterprise operation, it was adopted a communication infrastructure able to deal with and integrate all the available communication and information security technologies, creating a flexible and open subsystem (Osório, 1998).

## COMMUNICATION PROTOCOLS AND STANDARDS

There are several protocols available at different communication levels designed to specific or even general applications domains. Some of these protocols are being discussed inside standardization bodies like IETF, ISO/IEC, CENELEC, and ITU, among many others.

Organizations like the Internet Engineering Task Force (IETF) involves well-positioned computer industrialists, committed to achieve a general acceptation to some of their technologies (Dowd, 1996). In fact, there is a panoply of protocols addressing common application domains what creates extended complexity on how to deal with all of them. This section aims to present a survey of some of the most relevant protocol suites, considering its importance as enterprise information exchange supporters. The strategy adopted in the PRODNET communication infrastructure involves the integration of several of such protocol suits as basic communication resources among enterprise nodes.

### The communication protocols and the OSI reference model

The well-known OSI seven-layer reference model with its communication services is the main reference to almost all communication infrastructures. Some protocols have played an important role in the development of standards. The TCP/IP is one of the most important for its relation to the origin of the well-known Internet paradigm.

Furthermore, almost all-upper level protocols such as POP3, SMTP, FTP, etc., are based on TCP/IP. The Figure 1 shows a simplified view of the OSI reference model and the relative position of some of the mentioned protocol suits.

The TCP/IP suit is the support kernel to the communication among hosts implemented at the operating system level. This protocol suit has been extended to almost all the operating systems. The Windows NT implements the WINSOCK defined by Microsoft to guarantee interoperability with the Unix systems that firstly implemented the socket entity. As a matter of fact, several protocols emerged above TCP/IP using either TCP or UDP or both transport protocols, giving users, through dedicated applications, extended facilities to exchange or access information remotely. There is a trend for user applications to incorporate different communication protocols, providing to users simplified interfaces and extending their influence. One example of this trend is the integration into a Web browser of the ability to access web servers through HTTP, FTP servers through FTP protocol, and e-mail delivery and reception using POP3 and SMTP. This tendency is related with an expectation from users to have uniform applications to do different tasks without the need to call different tools each one with a specific interface and behavior, creating information consistency problems. An overview of some of the

mentioned protocols is presented, preceding the presentation of the PRODNET communication infrastructure.

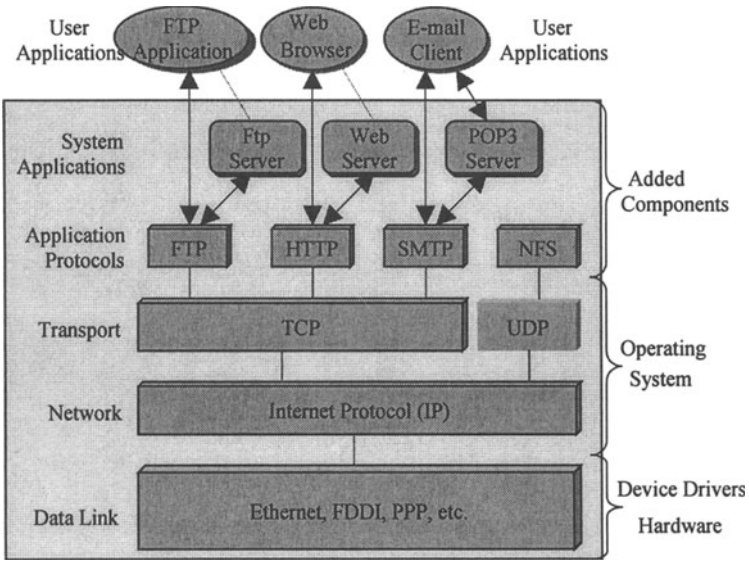


Figure 1 - Representation of the OSI layers

**File Transfer Protocol - FTP**

The file transfer protocol is widely used on the Internet for data files transference between host computers. With FTP, clients are able to login a server and download public files, even though they have not got local accounts. This anonymous client access facility has greatly contributed for the protocol's popularity. The FTP protocol is established through a TCP connection between the client and the server for command transfer. The commands are sent one at a time, or in other words, the reply must be received before another command is sent. The FTP needs to establish two different TCP connections for a file transfer. With this protocol it is also possible to use simultaneously multiple TCP connections, providing great efficiency in some network operations.

The control connection is used for client/server setup. The server receives client connection requests at port 21. When a client contacts the FTP server, they negotiate a typical TCP connection for data transfer purposes. This actual connection remains active during this session. The FTP protocol creates a separate data connection for each file-transfer operation. This communication resource involves three main components.

- user interface – user interaction commands;
- protocol interface – implements the FTP protocol itself;.
- data transfer process – data connection establishment and management.

The FTP can work with different operating systems, file structures, and character sets. A group of protocol options enables FTP to deal with different file formats.

**The Internet E-Mail**

The Internet electronic mail is one of the most used applications to exchange enterprise / personal information. In fact, about one-half of all TCP established connections are used for sending and receiving e-mail messages.

Although the e-mail service is mainly used for transferring text messages, it is also possible to use extended formats like the Multipart Internet Message Extensions (MIME) to embed into the message binary data such as graphic images, audio, and video files. A network e-mail system is made of few basic components:

- a message queue;
- the sender MTA - Message Transfer Agent;
- the receiver MTA;
- one or more mailboxes.

When a user wants to send a mail to a friend, he/she uses a user agent (UA). This is an application program that interacts with the e-mail system by putting mail on the message queue. Then, the sender MTA reads and sends it to the network. On the receiver part, the host receives the mail and, depending on its destination address, the message is put on the correspondent mailbox.

The user-interface is often an integral part of the e-mail system, but it can also be a separate client program that uses a client/server model to interact with the e-mail system, providing a user-friendly interface.

The MTA acts as an agent on behalf of a host computer, by shielding it from a wide variety of user agents or other MTA. Its main task is to route the message in the network, using the "envelope" information included into the message. As soon as the user agent sends an e-mail message to a message queue, the MTA retrieves the message and transmits it to another MTA depending on the routing strategy. This process continues until the message reaches its destination address. The communication between MTA is done through a TCP connection and using the SMTP protocol.

**Other e-mail exchanging protocols**

The X.400 standard from ITU defines a set of entities and protocols at different levels to exchange messages among different computer hosts. It has some extended characteristics like an embedded authentication mechanism that makes it more powerful than the Internet SMPT counterpart. However, due to its extended complexity and the existence of several incompatible implementations, it is used manly in large organizations. The emergence of the Internet e-mail with a simpler addressing mechanism has relegated it to a second plan.

**The e-mail account manager**

The Post Office Protocol POP3 aims to manage e-mail accounts on behalf of users accessing it through a User Agent (UA). The server keeps accounts and mailboxes

for all clients and uses a specific protocol for client/server communication. A POP3 access session involves three kinds of operations: authentication, transaction, and update. The authentication phase starts as soon as the client/server TCP connection is established, in the well-known port 110. In this phase, the user name and password is given to the server so that it can authenticate the accessing user. The users must start sending a message type USER, indicating the name, followed by a message PASS, with the access password.

Once the user authentication succeeds, the server locks the appropriate mailbox and the POP3 session enters the transaction phase. During the transaction phase, the user can obtain message information like the number of messages available and their size, the selection of a single message to retrieve, and other specific information. The user can maintain the connection, until the QUIT message is issued. This command force the POP3 session to enter into the update phase, consisting on removing all messages marked as deleted, unlock the mailbox, return success to the user, and finally close the connection.

**The World Wide Web infrastructure**

The World Wide Web or simply Web infrastructure is physically composed by a large number of Web servers located around the world. Each Web server contributes with a portion to the information that can be globally accessed creating a global and distributed information base. From the communication infrastructure point of view, the WWW got great popularity because it created an opened infrastructure dealing with several file formats and an easy way for users to access valuable information. The basic components of the Web infrastructure are: 1) the Web servers, located by default at port number 80; 2) the HyperText Transport Protocol HTTP, to rule the relation between Web clients and the Web servers; and finally, 3) the HyperText Markup Language HTML, to structure the information into files directly browsed by a Web browsers.

**The HyperText Transport Protocol - HTTP**

Any application wanting to access a Web server might follow the HTTP protocol, which involves operations like a connection, a request, a response, and a close. When a Web browser requests an HTML document from a Web server, the connection is open, the document is transferred, and then the connection is closed. For each new request, a new TCP connection is established. The extended characteristic of this protocol relies on the capacity to deal with differentiated information types like sound and images, among many others.

**The HyperText Markup Language - HTML**

An HTML file looks like a text file with several mechanisms directing the Web browsers to behave accordingly. This includes the management of links inside a specific document and the access to a Web server when references are encountered. The basic entities identifying resources on the Web are: the Universal Resource Indicator URI, that uniquely identifies a resource file; the Universal Resource Locator URL (<protocol>://*<host>*:*<port>*/*<path>*) including information about the

protocol and the server, that together with the URI are able to name uniquely any entity on the Web.

### The Common Gateway Interface - CGI

The CGI infrastructure (Gundavaram, 1996) was created to provide Web browsers with a mechanism to access HTML pages generated in consequence of an access. When a Web server receives an URI reference pointing to an executable file it starts a new process, the CGI-process, giving it information about the current access and some parameters identifying the Web client. The started process is supposed to produce an HTML file and send it back to the Web server, which delivers it to the Web client. One of the main advantages of the CGI infrastructure was to give Web servers the possibility to deliver HTML pages generated "on the fly" with information obtained dynamically from a database or other information source. One interesting characteristic offered by CGI is the possibility of answering according to the country location of the Web client or other specific characteristic requiring differentiated answers, different languages, different contents, etc.

Considering that all the communication protocols aim to transport information from one computer to another, local or somewhere in the global network, let us consider all of them as communication resources. An application can access any of these communication resources through some access port or either through some application programming interface, with access functions implemented in a static or dynamic library or methods of some object or component. From this brief synthesis, one important aspect to retain about the mentioned communication resources, is the need for an increasing integration to make them transparent for the users, when they use specialized software tools to support their jobs.

### Other Infrastructures Targeted to Client-server Based Systems

The RPC, the component/object model CORBA, the COM/DCOM, and the RMI are technologies created to facilitate the development of client-server applications, as they hide the low level communication mechanisms, like the transport protocol selection, the service identification, the security mechanisms, the computer platform heterogeneity, and so on. With these technologies, the programmer accesses remote services as local function calls, in the case of RPC, and as a method from an object or component in CORBA or COM. The difference relies in the calling semantics, instead of the "exactly once" semantics for local service calls, the "at most once" or "at least once" semantics have to be considered for remote services. Nevertheless, for the PRODNET communication infrastructure the relation among enterprise nodes does not follow a client-server model.

## COMMUNICATION AND INFORMATION SECURITY

### Security Mechanisms on Virtual and Open Worlds

The credibility of a communication infrastructure deeply relies on the quality of security procedures it implements. The main procedure to avoid pirates from

accessing transported information is to cipher it. Cryptography has played an important role in many circumstances. The oldest reference to cryptography goes back to the year 2000 B.C. - ciphered funeral messages were found in stones (Garfinkel 1996). Julius Caesar used a simple cipher technique to secure communications between Gaul and Rome. Caesar's cipher is based on a simple character shift of the transmitted message, three positions to the right in relation to the alphabet, see Figure 2. If the message carrier sleeps somewhere under a tree shadow and meanwhile an efficient spy makes a copy of the ciphered text, the enemy would have some trouble to discover the clear text (the original message).

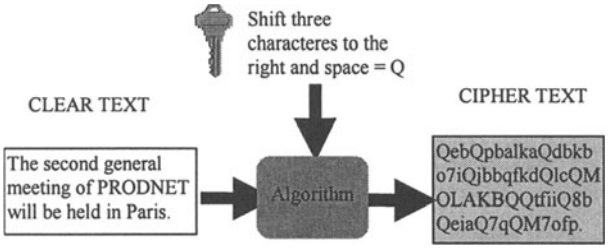


Figure 2 General cryptographic model

This kind of cipher, referenced as **substitution cipher**, is not sufficiently robust against the new kind of attacks based on powerful computational systems. Several cryptographic techniques exist nowadays, most of them based on intensive utilization of computational resources, which strongly difficult the task to hide clear information.

This topic aims to give an overview of the main concepts related with security, including the equation of the main problems that the security infrastructure must solve. It will survey some of the most up to date techniques applied to secure information exchange through insecure communication channels. The actual openness of enterprise internal computational facilities to Internet or other outdoor communication support imposes an extra effort to avoid unauthorized private information accesses.

Enterprises need to believe that their information systems are secure enough to avoid all kind of threats, or at least, to be able to send warnings when someone is perpetrating an attack against some part of the information system infrastructure.

## The Security Infrastructure Main Goals

To understand the mechanisms that a security infrastructure must support, let us start with the definition of some basic concepts.

Privacy threats to information repositories, or during information transmission, can take many forms. To clarify the principal security problems (Colouris, 1994) classifies threat methods into four classes:

- ***leakage*** - access to information without authorization;
- ***tampering*** - alteration of information without authorization. This includes the exchange of programs behavior (through virus, mobile agent, etc.);
- ***resource stealing*** - unauthorized utilization of resources;

- ***vandalism*** - information forge without any gain to the perpetrator.

In fact most of the above classes of threats can provoke big damages to an enterprise. One possible scenario would be the reception of a big (false) order, which makes the enterprise owner happy, but unfortunately coming from someone that just wants to reduce the concurrency. This situation can also happen when transactions have human intervention. The security does not depend on the way business is made but on security measures.

Considering the threats classification presented above, the security objectives can be grouped into five categories (Macgregor, 1996):

- ***access control*** - locally or remotely accessed services should be validated against unauthorized users. This can include the permission validation to do a specific information access;
- ***authentication*** - it is necessary to be sure that the interlocutor at the other side (human or computer process) is what it claims to be;
- ***integrity*** - it is necessary to believe that the information received is what was sent;
- **non-repudiation** - it is necessary to guarantee that the sender and/or receiver do not cancel the transaction after it took place (accountability);
- ***privacy*** - eavesdroppers should not have access to sensitive information.

Any security infrastructure must be aware of the panoply of attacks, some of them using unimaginable approaches. To better understand how information systems can be threatened (Macgregor, 1996) classified attacks into three classes:

- ***passive attacks*** - the perpetrator monitors the information traffic, trying to infer useful information. This kind of attacks can be directed to the communication infrastructure or else to the computational systems. One form of eavesdropping can include the offer of a *"Trojan horse"* (some corrupted software component, maybe with an unknown virus) to redirect useful information to the eavesdropper;
- ***active attacks*** - this kind of attack tries to break through systems defense:
  - the attacker tries to enter into the system, to discover security characteristics and gain control of some client or server;
  - the attacker presents himself to the system as a trusted user, trying with this behavior to get secret information and more trustees;
  - with cryptographic attacks, the attacker tries to get access (discovering passwords) and/or decrypt information.
- ***denial of services attacks*** - a worst situation can result from the substitution of some services by dirty ones or send big amounts of trash information to the enterprise.

**Evaluation of Existing Methods and Procedures**

The security of information transmission or prevention against unauthorized service accesses is not an easy task. The actual computational capacities impose enhanced techniques to prevent threats against enterprise information system.

There are two main techniques offering such capabilities. The oldest one is the ***Secret Key Cryptography*** (Smith, 1997) technique, also known as *symmetric cryptography* (Schneier, 1996). A more recent technique is the ***Public Key Cryptography*** (also known as a*symmetric cryptography*). With private key cryptography, messages are encrypted using a key that must remain secret to everybody except to both the sender and the receiver.

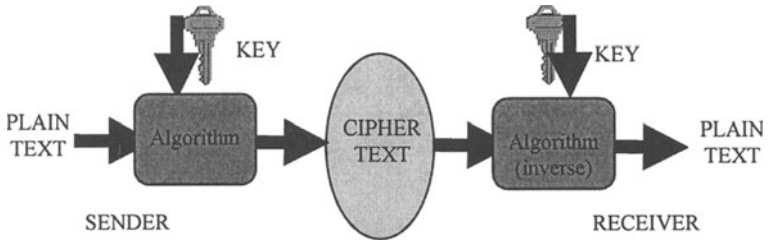


Figure 3 - Secret key cryptography model

Some of the well-known algorithms used to generate ciphered text using a symmetric key are the DES, the Triple-DES, the RC2, and RC4, and also the IDEA algorithm, among many others.

The key distribution and authentication are the main problems when using private key methods. It is mandatory to be sure that our interlocutor obtained the secret key, maybe from some key distribution server. The system Kerberos developed at MIT (Colouris, 1994) implements an authentication protocol with key distribution facilities. The Key Distribution Center (KDC) (Garfinkel, 1996), is another interesting infrastructure to support private key distribution.

The public key cryptography is based on two keys, one published and the other remains private, see Figure 4. Someone that wants to receive information, only known by his/her friend and himself, must generate two keys. One of the keys, the public one, must be put on a public repository and its finger print into a presentation card. The other key, the private key, must be kept in a safe place and used only to decipher the received messages from the friends.

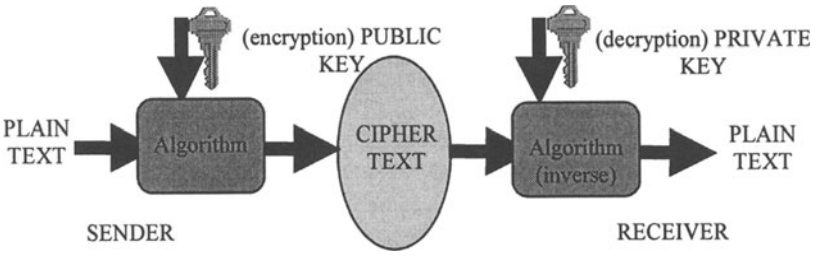


Figure 4 - Public key cryptography model

With public key cryptography the key distribution problem does not exist. A well-known algorithm to generate a key pair is the RSA (Rivest, Shamir and Adleman) algorithm.

Another advantage of public key cryptography is the support to the ***Digital Signature***. Beyond authentication, the communication infrastructure must provide legal commitment of the sender. If someone sends an order and later on nobody assumes that act, someone must undoubtedly be indicated as responsible (legally) for that operation.

This commitment is done using a special function, a digest function (a secure hash function, a kind of check sum) to generate a characteristic value derived from the plain text (the clear message). This fixed length characteristic value must be different for each different message generated by the sender and it must not be possible to generate the original message. The MD5 algorithm proposed by Rivest, is an example of such a digest function broadly used in several protocols.

Encrypting the fixed length characteristic value with the secret key of the sender generates the digital signature. The receiver only has to decrypt the fixed length characteristic value with the public key, published by the sender. If the digest function applied to the received plain text generates the same fixed length characteristic value, the receiver has legal assurance that the message came from the expected sender.

### Standards Toward a General Interoperability

There are several systems that implement some of these encryption techniques, at the application/system level, like the Pretty Good Privacy (PGP), Privacy Enhanced Mail (PEM), and the Kerberos, among many others.

There are other protocols with security features (most of them built from scratch and others resulting from enhancements to existing ones), such as: Secure Socket Layer (SSL), Privacy Communication Technology (PCT), SHEN - proposed by CERN to enhance web security, Secure Transaction Technology Protocol (STT), Secure Electronic Payment Protocol (SEPP), Secure Electronic Transactions (SET) (Loeb, 1998), (SET Book 1, 1997), Public Key Cryptography Standards (PKCS#), Secure Hash Standard (SHS), Secure HyperText Transport Protocol (SHTTP), Digital Signature Standard (DSS) (Federal Register, 1991), among others.

### Guarantees Offered by Security Technologies

A generalized debate about security issues and what should be the best security framework is going on, offering to people the privacy they deserve and to the police detectives the correct mechanisms to investigate criminals.

The problem is so complex that some experts argue that cryptography is not the main security issue to be considered. For the business, one important concern is to have a good authentication framework, providing auditing information with an integrity seal – with legal support.

Most of the well known cryptographic algorithms, both for symmetric and for asymmetric cryptography, are good enough to guarantee a high confidence degree.

The computational effort necessary to attack privacy guaranteed by secret or public key algorithms is so high, that it is not a main concern for business.

**Worldwide Initiatives Concerning Security**

There are many worldwide initiatives addressing the information security issues. In this chapter some of the most significant activities concerning the discussion of the most relevant aspects of security are presented. Even if some of them have a global approach, an attempt is made to group them by world blocks or by country.

There are several initiatives concerning the establishment of a global and interoperable framework to support secure electronic communications. The recent recommendations the OECD (Organization for Economic Co-operation and Development) advise government members to adopt country level policies conducting research and development in order to achieve such global market (Anderson, 1995), (Taylor, 1997). The principles stated in the report (OECD, 1997) show some important issues related with security:

- **trust in cryptographic methods** – trustworthy in cryptographic methods is essential to generate confidence in the utilization of information and communication systems;
- **choice of cryptographic methods** – users should have a right to choose any cryptographic method, subject to applicable laws;
- **market driven development of cryptographic methods** - cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments;
- **standards for cryptographic methods** - technical standards and protocols for cryptographic methods should be developed and promulgated at the national and international level;
- **protection of privacy and personal data** - the fundamental rights of individuals to privacy, including communications secrecy and personal data protection, should be respected in national cryptography policies and in the implementation and use of cryptographic methods;
- **lawful access** - national cryptography policies may allow lawful access to plain text or cryptographic keys hiding encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible;
- **liability** - whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated;
- **international cooperation** - governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove or avoid creating, in the name of cryptography policy, unjustified obstacles to trade.

These principles are grounded on the recognition that the cryptographic techniques can offer the right mechanisms to guarantee the basic security requirements like integrity, privacy and authentication, for information access, communication networks and systems in general. The main problems are on the

establishment of a global and interoperable framework providing to individuals and systems a secure information store and communication infrastructure. However, the domain addressed by PRODNET II is much more restricted: enterprises with PRODNET II software are implicitly certified and the Web door is planned to be a very restricted information access.

## THE PRODNET COMMUNICATION INFRASTRUCTURE - PCI

The PRODNET project, beyond other more general objectives, aims to offer enterprises a communication infrastructure satisfying the most important requirements needed to support their business relations, which are:

- any sent document is exclusively received by the destination enterprise. No one else can access to the sent document – **privacy**;
- the receiver enterprise can be sure that the received document is the same that has been sent and no one else can read or change it – **integrity**;
- any received document can be univocally related to an identifiable sender – **authentication;**
- depending on the contracted communication services, the availability does not depend on the failure of a single communication resource. Only when all are inoperative, there is no enterprise communication at all – **availability**;
- the sender should be able to retain a receipt proving in court that the receiver really has received a document. On the other hand the receiver must be able to prove that the identified sender has sent a given commercial document - **non-repudiation**;
- audit information about all sent and received documents is maintained to ulterior evaluation in front of some communication problem or any legal request for clarification – **auditing**.

The quality of the services, offered by information technologies to deal with their valuable business information, is the main concern entrepreneurs have when evaluating the adoption of new technological solutions. At the head of the quality concerns is the availability of the technological solutions (hardware and software). If the business depends on technological solutions, there is no space for integrity faults, information losses, privacy violation, operational failures and other quality violations. With the PRODNET Communication Infrastructure - PCI - some of these concerns are solved. The PCI offers to an enterprise node a technological component guaranteeing as much availability it is possible to provide, based on the communication resources quality.

There are, however, some aspects not addressed by PRODNET II that are also very important to get the entrepreneurs confidence. The legal implication is one of them as it will be mentioned later. However, even if it is important, it is not the main obstacle to have a general entrepreneur acceptation. Even if there are some risks making electronic business without a legal framework supporting it, the real systems have always a positive approach to this kind of possible problem. The need for evidence to prove something that was wrong is the exception and the real business is not based on a one hundred percent safe framework. It is, however, necessary that

enterprises and law makers understand and trust the extent of technological facilities to be able to produce a new generation of laws adapted to the reality of the electronic market.

The utilization of a public and untrustworthy space as the communication infrastructure connecting enterprises requires extra mechanisms to transform such open spaces in a secure communication path. The Internet as an open space has the advantage of being cheaper. However, as more open is a technology more vulnerable it is to attacks perpetrated by experts with a distorted mind. The PCI aims to provide the PRODNET infrastructure with a reliable and secure communication service. The quality of the communication services is improved providing redundant communication resources with a flexible management. Besides communication, the security framework guarantees the trust required by enterprises to protect their business. Considering the emergence of the Web infrastructure, PRODNET includes also a Web client access supported through the CGI protocol.

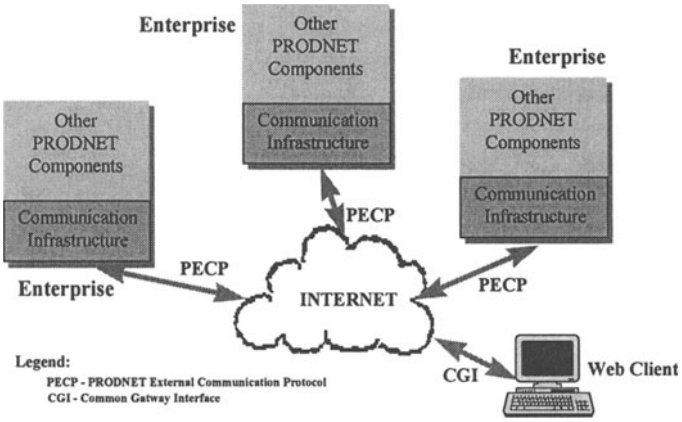


Figure 5 - PRODNET communication infrastructure

The main characteristics offered by the PCI subsystem are:

- ***communication availability*** – depending on the communication resources (communication stacks positioned at different levels) the messages will be exchanged considering the best quality of service. The message delivery fails exclusively when none of the available resources is operative. The user quality specified service has precedence over the heuristics used by the PCI communication manager. To increase availability, the message receipts can use a different communication resource of that used by the original message;
- ***communication security*** – message privacy, integrity and authentication is guaranteed. Independently of the selected communication resource only the sender and receiver can access the clear exchanged message, any change in the message content is detected in the peer node and both sender and receiver can prove the identity of each other. The effectiveness of these features depends on the user quality of service specification;

- ***communication with legacy systems*** - messages originated from nodes without PRODNET software can be delivered to a PRODNET node using a general-purpose e-mail client (SMTP/POP3 compliant) like Eudora, MailExchanger, or others. On the other hand, any PRODNET node can send e-mail to an account not controlled by the PRODNET software. In the former case the delivered message may include some human interpreted data or else data interpreted by some software tool (EDI parser, STEP files processor, etc.);
- ***secure access from a Web client*** – a general infrastructure enables Web users to access PRODNET information considering the achieved authentication level. Depending on the ability for a Web user to provide his/her/it certificate (*it* refers to process/application), the PCI will adjust the access level accordingly. For accesses not authenticated, the PRODNET system only makes available public information (the enterprise profile or its home page for demo purpose); for accesses strongly authenticated, the created secure channel can access private information. The PRODNET Web access uses the CGI infrastructure with security enhancements.

**The PCI architecture**

The PCI component provides a deliver message service considering the best unification between other PRODNET modules communication expectation and the real available communication resources.

The PRODNET Intelligent Communication Manager (PICM) is the main component of the communication architecture. The connections (message exchange) among enterprise nodes present transparency to temporary failure of some of the available communication resources. It is also a task of the PICM module the supervision and control of the communication logical links. Log information is maintained to support monitoring operations and to help communication module to decide on the selection of the best communication resource that guarantees communication requirements (time to deliver the message). The lowest level of the communication infrastructure makes the virtualization of the different communication resources.

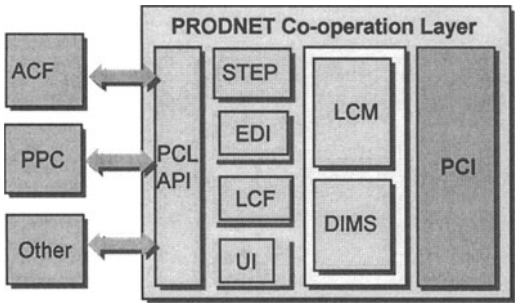


Figure 6 - The PRODNET architecture

Three communication resources were selected for the prototype evaluation: a low-level TCP/IP link, the SMTP/POP3 e-mail message exchange, and also a WEB door based on CGI protocol. The CGI protocol will support the connection of Web clients accessing valuable PRODNET information. The communication among enterprise nodes is exclusively supported by a TCP/IP connection and a SMTP e-mail messages. The PRODNET External Communication Protocol (PECP), a PRODNET proprietary protocol, is used to support messages flow among enterprises. Besides communication, a security framework provides PRODNET architecture with the necessary security mechanisms.

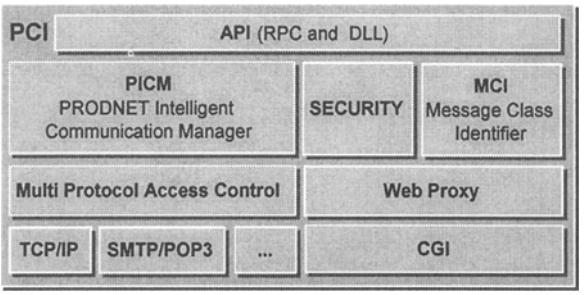


Figure 7 - The PCI General Architecture

The Figure 7 presents the PCI architecture with its main five components:

- the **PICM** aims to manage all communications guaranteeing as much availability as it can;
- the **Multi Protocol Access Control** (MPAC) guarantees communication resource transparency to the PCIM module. The addition of another communication resource has only implications at MPAC level. A general communication resource interface and description is managed by MPAC module. This module also deals with specificity of each communication resource (max message dimension, etc.);
- the **Security module** will implement information message privacy, authentication and integrity. Further details about security framework are presented in the next chapter;
- the **Web Proxy** implements the access from a general purpose Web browser based on the CGI protocol. This communication protocol does not follow the generality presented by the other selected communication resource. The CGI is limited to present Web clients a secure access to PRODNET information;
- the **Message Class Identifier** (MCI) aims to manage the reception of messages from legated systems. Those messages received into the PRODNET kernel e-mail account are processed to determine its content type. Depending on their type, the respective PRODNET module is called, following a specific workflow plan.

All of the PCI services are available to the other PRODNET modules through a DLL following a client-server model. The calling modules are signaled when the

delivered messages arrive as planned. If some exception happens the client modules are reported about them.

**The Security Module**

The PRODNET Security module provides message privacy during message transportation, through the utilization of both the mentioned cryptographic techniques. The receiver enterprise node public-key is used to cipher a session key.

This session key is randomly generated for each message to be delivered, (see Figure 8) and used to cipher the message content. The receiver node starts to retrieve the session key from the received message, using its private key to decipher it. With the session key, the receiver node can obtain the original message content. However, with this schema it is not possible to guarantee that the message was not changed during its transportation. Another important aspect to be considered is the authentication of the sender.

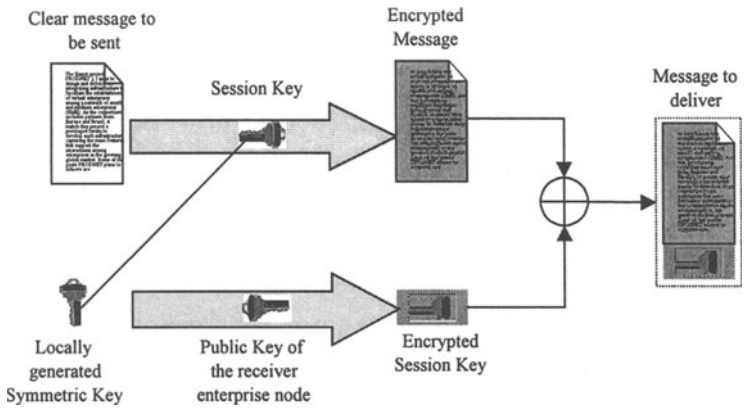


Figure 8 - Encryption technique used to guarantee privacy

**The Authentication Framework**

The authentication is being done in the Security module. Depending on information access restrictions, authentication is done to legally validate the message sender. The authentication is mainly based on the digital signature paradigm and on certificates managed by the PRODNET software.

The PRODNET authentication involves the inclusion of a digital signature in the sent message. With this digital signature, the receiver can check if the message was changed and, furthermore he can legally associate the message to the sender, considering that the public key was checked against the corresponding certificate. The digital signature is generated, encrypting the result of the digest function applied to the message content, with the sender's private key. The receiver node can verify the integrity of the message and the authenticity of the sender by generating the digest message and compare it with the received deciphered digest message. The receiver node is able to detect any information tampering (see Figure 9).

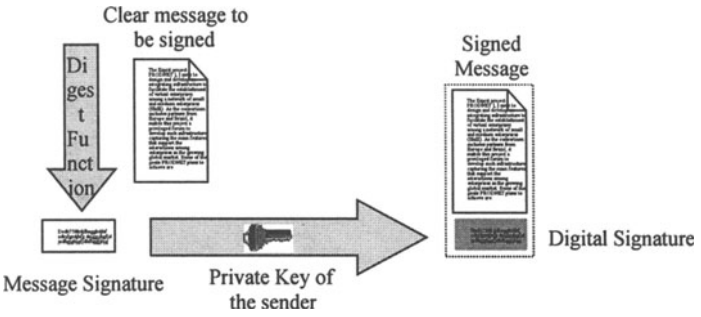


Figure 9 - Generation of the digital signature

With these services, PRODNET will provide virtual enterprise nodes with a private communication infrastructure, enhanced with authentication facilities.

Authentication is crucial when the communication infrastructure supports exchange of commercial information. No one can repudiate a message that was signed and sent by one enterprise node. In the future, the PRODNET communication infrastructure must be trusted against some communication authority in order to guarantee that some repudiation can be tracked and that is valid to be present in a court.

**The PRODNET Web Proxy**

Considering the emergent Web utilization for secure operations, it was also considered into the PRODNET architecture an access from a standard Web client.

Any one with an Internet connection can access to a PRODNET enterprise node selecting the specific URL address and giving the required authentication information. The connection is done through a gateway process started by the accessed Web server. This CGI process guarantees the communication between the PRODNET Web proxy and the Web client. In the first accessing phase the Web proxy authenticates the user client and depending on the presented credentials it decides what will be the user's access level. When authenticated, it is established a logical private channel between the Web client using a standard Web browser and the PRODNET node (see Figure 10).

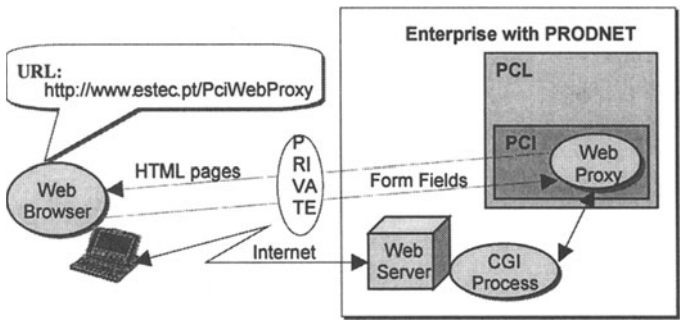


Figure 10– The PRODNET Web access door

The private logical channel established from a Web client to a PRODNET node is based on the particular PRODNET certification framework. Depending on the capacity of the Web client to give certifying information according PRODNET framework, the information access level is conditioned. Before acquiring confidence a client must give PRODNET network information about how to authenticate him/it. As it happens with Web clients, as well as with e-mail messages received from enterprises without PRODNET, the authentication is based on the credentials given by the message sender.

**Electronic Information Exchange Risks**

The trustfulness of the PRODNET infrastructure is based on the credibility of the PRODNET software components and on the trustworthiness of the enterprise network members.

The credibility of the PRODNET software is guaranteed by an initial challenge based on a set of secret keys created at the installation phase, to confirm if the software is original. Even if someone tries to replicate the PRODNET software accessing technical information, all legal software copies can detect this situation. This key is also used to guarantee that PRODNET software is always associated with a specific enterprise.

Based on the confidence of software components, the next step is to certificate if the other enterprise is who it claims to be. During the PRODNET installation process it is associated a X509 compliant certificate generated by PRODNET vendor or integrating the existing enterprise certificate. This certificate might be used for other purposes than the enterprise authentication to PRODNET.

However, even if many security measures are taken, there are always sets of risks that entrepreneurs have to face when deciding to enter an enterprise network. Nevertheless, considering the risks faced nowadays by entrepreneurs when dealing with paper based business, a good security framework can provide electronic commerce with an extended set of security/preventive facilities. The new risks can be classified into the following classes:

- **authentication failure** – this is somehow the worst security risk. Giving confidence to someone who is not who he announces himself to be, might bring the enterprise to a set of troubles with liability implications;
- **privacy violation** – someone accesses enterprise restricted information what can compromise some important business;
- **legal framework and liability** – even if this is not a main risk it is important to provide a legal support to the electronic business and to provide legal evidences to track business transactions done, in order to clarify disagreements;
- **availability failure** – if business is deeply dependant on some infrastructure, any failure can be transformed into business losses. The integrating infrastructure that supports business becomes an enterprise strategic resource;
- **business vulnerability** – the track of information/messages exchanged among enterprises, can offer to competitors strategic information. If the list

of the partners of some enterprise is known, important facets of its business strategy can be inferred.

Most of these risk classes are interrelated. As an example, for the legal framework it is very important to trust in authentication and information integrity. It is necessary to prove that stored log information was not tampered. If a failure results on log information lost, it will be not possible to track the electronic business done and subject it to an evidence research. If the hardware and system software is not certified (totally secure), PRODNET can not provide complete security, authentication and integrity. If a "Trojan horse" inside the PRODNET host access the information and delivers it in clear to some place, where it is collected and processed, nothing can be done to prevent it to happen.

This is really a complex subject and a complete solution is not easy to achieve. The PRODNET's strategy is to be aware of the main problems related with security in a wide sense and to integrate into the architecture the state of the art in this domain. Besides this, a complete auditing information is maintained, to provide an "intelligent" continuous evaluation of the platform behavior. Continuous monitoring of PRODNET communication infrastructure will provide the system manager with supervision valuable information.

## CONCLUSIONS

The last developments in computing and communications have established several *de facto* standards, creating many difficulties when the goal is to offer a global infrastructure presenting a good level of users satisfaction.

The reality is made of several heterogeneous components creating to enterprises added difficulties to manage their information in a consistent and uniform way. The PRODNET communication infrastructure contributes to make possible for SMEs and other enterprises the establishment of their electronic cooperation channels based on service quality and security. Beyond technology, one important factor contributing to the information security relies on a set of procedures all enterprise managers and employees might follow in order to avoid security cracks. The legal implications associated to the electronic business are deeply related with organizational weaknesses. Nevertheless, PRODNET offers a set of services and tools that will contribute to manage the enterprise electronic business, offering mechanisms to detect and evaluate communication and security failures.

### Acknowledgements

This work was done in the context of the PRODNET II project, partially funded by the European Commission. The authors thank the valuable contributions from the consortium partners: UNL (P), CSIN (P), UvA (NL), UFSC (BR), ProSTEP (D), UNINOVA (P), MIRALAGO (P), HERTEN (BR), LICHEN (F), and ESTEC (P).

## REFERENCES

1. Anderson, B. J. Crypto in Europe – Markets, Law and Policy, 1995.
2. Coulouris, G., Dollimore, J., Kindberg T. Distributed Systems, Concepts and Design. Addison-Wesley, 1994.
3. Dowd K. Getting Connected, O'Reilly & Associates, 1996.
4. Federal Register. Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), v. 56, n. 169, Aug 1991.
5. Garfinkel S. PGP - Pretty Good Privacy. O'Reilly & Associates, 1996.
6. Gundavaram S. CGI Programming. O'Reilly & Associates, 1996.
7. Jamsa, K.; Cope, K. Internet Programming. Jamsa Press, 1995.
8. Macgregor, R. S., Aresi, A., Siegert, A. WWW.Security, How to Build a Secure World Wide Web Connection, IBM, Prentice Hall PTR, 1996.
9. OECD – Cryptographic Policy: The guidelines and the issues (The OECD Cryptographic Policy guidelines and the Report on Background and issues of Cryptographic Policy, OCDE/GD(97)204, Paris, March, 1997.
10. Osório, A. Luís; Gibon, Pierre; Barata M. Martins. Secure Electronic Commerce in Virtual Enterprises of SMEs, presented at the international conference BASYS'98, 27-28 August 1998 in Prague and published by Klower, 1998.
11. Schneier, Bruce. Applied Cryptography. 2nd edition, John Wiley & Sons, 1996.
12. SET Book 1. SET - Secure Electronic Transactions Specification, Book 1: Business Description, Visa and MasterCard, May 1997.
13. Loeb Larry. Secure Electronic Transactions: Introduction and Technical Reference, Artech house Publishers, 1998
14. Smith, Richard E. Internet Cryptography. Addison-Wesley, 1997.
15. Stross C. The Web Architect's Handbook. Addison-Wesley.
16. Taylor, I. Minister for Science & Technology. Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation, March 1997.