OPEN SECURE MODEL AND ITS FUNCTIONALITY IN NETWORKS WITH VALUE-ADDED SERVICES

Borka Jerman-Blažič
Jožef Stefan Institute, Jamova 39, Ljubljana, Slovenia
Phone: +38 61 159 199, Fax: +38 61 158 058

Keywords: security mechanisms, kryptography, networks, value-added services

Edited by: Rudi Murn
Received: December 12, 1992 **Revised:** February 9, 1993 **Accepted:** March 1, 1993

The contribution gives an overview of the security functions employed in the Value Added Networks technology. The overview represents briefly the user requirements for secure communication, the basic threats to which communication systems are exposed and the framework of Open Secure Model defining the security functions and services to be used in an open network. The security mechanisms used for provision of the security services and functions are briefly described. Several applications used in Value Added Networks with inbuilt security functions are briefly introduced at the end.

1 Introduction

Information gains value once it is exchanged or consumed. To be exchanged or consumed it must be transferred or delivered. The need for effective and safety means of carrying this process is today growing faster then the growth of information and electronic data processing. Nowadays, information interchange and data communication is an integral part of any modern information system. Information interchange is a process taking part in the services offered through networks known as Value Added Networks or VANs. These networks usually interconnect communicating users with various information services.

Every VAN is different in its structure and the services it offers. Some of the services are very generalized and some are extremely specialised. A comprehensive VAN is likely to have the following general components [1]:

basic network,

generic services,

transaction relay,

application enabling,

information databases,

network management and help desk.

Generic services are general purpose services needed by a wide range of customers rather being application or industry specific. The main examples are electronic mail, bulk data transfer, Electronic Data Interchange (EDI) and information services support for managers or professionals.

VANs do not have to own a proper wide area network, but they generally do. At its simplest they might just provide point-to-point packet switching. At a more advanced level they may also offer protocol conversion to support a wide range of different equipment. Overall, their aim is to provide full connectivity between all the equipment and systems that their customers need. Connectivity and security are inherently contradictory requirements. However, with specially added security services it is possible to built open, fully connected network with any required level of security.

This contribution gives an overview of the security functions taken as a part of globally interconnected network. The overview deals with the user requirements for secure communication, the basic threats to which communication systems are exposed and the framework of the model which defines the security functions and services in an open network. The security mechanisms employed for the provision of the security services are briefly described. Several applications used in

Value Added Networks with inbuilt security functions are briefly introduced at the end.

2 Open networks and threats

Today, separate networks are integrated into a global connected network known as Global Internet [2] consisting of a number of interconnected networks. Individual computers and work stations are connected to fast Local Area Networks (LAN) spanning office building or parts of them. These LANs are usually connected into fast area backbone networks interconnecting one building, building complex or campus area at a speed comparable to that of LANs (100 mb/s). Metropolitan Area Networks are emerging. They will span entire cities with speeds above 100 Mb/s. Unlike LANs, MANs will be an integral part of the modern public network infrastructure being owned and operated by teleoperators and sharing the addressing and network management schemes of other public network. Wide Area Networks are used for long-haul services. Modern WANs are based on fibber optics transmission systems in the Gb/s speed range. All these networks today are not anymore separate physical networks but rather virtual networks, i.e collections of Network Service Access points (NSAPs) forming one world-wide logical network. One NSAP can simultaneously belong to any number of such logical networks. The protocol suites used in these interconnected logical network are mainly the Internet protocol i.e TCP/IP suite defined on the Request for Comment standards [3] and the OSI protocols developed within OSI Reference Model [4]. Upper layer ISO protocols can be run on the top of TCP/IP and vice versa, enabling the connected networks with different technology to provide global connectivity. Recently, the Connectionless Network Service and Protocol developed within ISO was adopted as an RFC standard and that among the other developed interworking techniques can be considered as step forward towards better coexistence of these technologies and provision of global connectivity.

Connectivity and security are inherently contradictory requirements. However, openness as is understood today does not mean lack of security but it means interconnectivity and the ability to interoperate between systems in different organizations and from different manufacturers. When an open distributed system is built up it becomes essential to define the user requirements regarding the security of communication. The users, depending on which service of the communicating system are they using may require different level of security. Usually, users are concerned with the following:

- the identity of the other communicating party,
- that nobody else can listen to the session,
- that nobody can undetect delete from, change or add to the information they are interchanging with other party,
- that commitments made during the session can beyond reasonable doubt, afterward be provided to an impartial judge.

The user apprehensions come out from the fact that the communication systems and resources connected are usually targets of different threats.

The threats can be oriented towards the communication network itself or towards unauthorized access to local system where the communication network is used only as a medium of access. So, three categories of assets within a globally interconnected network can be identified, the manipulation of which is a serious threat:

- the resources in the network,
- the informations conveyed
- and partner relations.

Local systems are resources accessed through the communication system and they must be protected. The communication system itself is a resource and must be protected too. The users of communication systems expect the communication system components to be present and to function and in that sense, the availability of services and stability of services are also the assets of the communication system and need protection.

Informations are the actual content of communication. Unauthorized access to informations, both by eavesdropping and by damaging, can destroy the value of information. Informations held locally and accessible through communication media also belong to that category.

The relation between communicating partners is another basic asset of communication. Without trust in the authenticity of a communicating partner all communication with is worth nothing. Trusted partner relations are characterised by: the trust in the identity of the partner and the trust in the actions of communications.

All the assets of the communication system are exposed to two fundamentally different kinds of threats i.e intentional or not intentional. In the classical security technology only one type of threats is considered i.e the intentional threats represented by the act of espionage and sabotage. Espionage comprises all passive intentional threats such as to get unauthorized knowledge of confidential or classified information. Sabotage comprises all active intentional threats i.e all kind of unauthorized manipulation of data, access to the resources to the communication system etc.

The other potential accidents which are also regarded as security relevant in the communication networks are accidental threats such as bad maintenance leading to an interruption of the network services. From the point of view of the users it does not make any difference if this is caused by a malicious or by an unable administrator.

The various threats and attacks in an open environment are classified within the framework document of ISO (International Standard Organization) [5]. This document (ISO -7498 part 2) identify five different attacks to the open communicating system i.e :

- masquerade,
- repudiation of action or service or,
- denial of service.
- data interception
- data manipulation

a. Masquerade can happen during the mutual validation of the message transfer agent (MTA is an entity which transfer/exchange messages in the electronic mail service) is by the exchange of the MTA names in plain text. An unknown MTA (for example in testing procedure) may be interconnected with some operational MTA by sending one of the known MTA names. This is a typical masquerade of identity with the intention to steal working resources or information. The masquerade of user identity is possible also by tricky handling of routing oriented addresses [6].

b. Repudiation of action or service: repudiation of origin, submission, or delivery of information is extremely painful if contracts or other business documents are considered. How to trust to an invoice received by an EDI service if no evidence of the sender identity can be provided?

c. Denial of services: denial of services can happen due to accidental interruption caused by local system failures or by nonconformant components in cooperating systems, such as erroneous entries in address routing or name mapping tables. Intentional interruptions are normal for maintenance purposes.

d. Data interception: the breach of confidentiality is the most common attack in the existing networks. It is impossible to guess the number of intentional espionage by system administrator or other unauthorised persons able to read data on their own or on other systems. Data may be intercepted also non intentionally in case of misrouted messages etc.

e. Data manipulation: is any kind of unauthorized modification of data and thus violates their integrity. The managing of electronic mail addresses is also in some sense a violation of integrity, accidentally caused by bad maintenance. This is obviously a case in gatewaying, electronic message get loss or cut of their bodies. This type of vulnerability of the communication system includes also manipulation of a message contents in the originator's local store after non-repudiation of submission and/or manipulation of message contents in the recipient's store after non- repudiation of delivery of the message.

The situation that communication services not being provable and that different security failures can happen in a globally interconnected network was acknowledged on many forums. Some of them spent a lot efforts to develop security functions and to provide security models. ISO has

addressed the security issue in several documents defining the Security Services or more properly the Security Functions in an Open Environment. General overview of the Open Secure Architecture is given in the Security Frameworks document [7].

3 Security functions and services

The Security Framework is intended to address the application of security services in an Open System Environment, where the term "Open Systems" is taken to include areas such as Data Bases, Distributed Applications, Office Document Processing and Communication Networks. This framework defines the means of providing protection for systems and objects within the systems and with interactions between systems. The framework address both information and sequence of operations which are used to obtain specific security services. These security services may apply to the communication systems as well as to the information exchanged between systems and to the local resources or data managed systems. The term security in the ISO framework is defined as "a mean of minimizing the vulnerabilities of assets and resources". Security is therefore understood as a system preventing the attacks and protecting the assets from the threats. Threats are therefore, encountered by security services implemented at different layer of communicating networks or within the user interfaces. Security services are implemented by employing security mechanisms. Some mechanisms prevent attacks, other detect attacks, some of the latter provide recovery of an unmanipulated state. They are:

Authentication: Many open systems applications have security requirements which depend upon correctly identifying the principles involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an identity based access control mechanism might be used, and/or for accounting and charging purposes. The process of corroborating an identity is called authentication.

Access control: Many open systems applications have security requirements which demand that resources be only used in a manner consistent with the prevailing security policy. The process of determining whether the use of resources within an open system environment is permitted and subsequently preventing such use is called access control.

Non-repudiation: the non-repudiation services ensures the proper collection and maintenance of information consisting of the origin or delivery of data in order to protect an originator against the false denial of a recipient that the data has been received or to protect a recipient against the false denial by an originator that the data has been sent.

Data Integrity: the maintenance of data value is actually its integrity. Many open system applications have security requirements which depend upon the integrity of information. Such requirements may include the protection of information used in the provision of other security services such as authentication, access control, confidentiality, audit and non-repudiation, that, if an attacker could modify them could reduce or nullify the effectivness of those services.

Data Confidentiality: Many applications have requirements which depend upon the secrecy of information. Such requirements may include the protection of information used in the provision of other security services such as authentication, access controls or integrity, that if known by an attacker, could reduce or nullify the effectiveness of those services. The maintenance of the secrecy of data is called confidentiality.

Audit: A security audit is an independent review and examination of system records and activities. The purpose of a security audit is an independent review and examination of system records and activities. The security audits: tests the adequacy of system controls, confirm compliance with established security policy, recommend any indicated changes in controls, policy and procedures, assists in the analysis of the attacks, and hence recommend damage control procedures. A security audits requires the collection and recording of security related events in a security audit trail. A security audit itself involves the

analysis and reporting of the information collected by the security audit trail.

Key management: In communication and information systems there is an ever increasing need for data to be protected against unauthorized disclosure or manipulation using cryptographic mechanisms. The security and reliability of such mechanisms is directly depended on the protection afforded to a security parameter, called the key. The purpose of the key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. Key management includes key generation, key distribution, key installation, key storage and key deletion. A fundamental problem in a key management is to establish keying material whose origin, integrity, and in the case of secret keys, confidentiality can be guaranteed.

The placement of particular security function in the Open Architecture is not exactly defined. Security services or functions may be provided by different layers and by different protocols depending of the user and application requirements. Some applications are more and some are less vulnerable. The protection of particular application depends also of the adopted security policy and on the technology used. It can be said, that no universal model exists and that the placement of particular function is chosen after the features and the requirements of particular application regarding security are identified and by pragmatic considerations.

For example, in connection oriented end to end services the transport connection is dedicated to serve one end to end instance of communication and for that reason any security function can be placed at the transport layer or between the transport and the network layer. There are several protocols that implement several security functions on that level i.e NLSP, SDNS, EESP and SP4 [7]. The placement of the function depends also on particular user requirement such as for example traffic flow confidentiality. This security function can only be reliable implemented at layers 1 through 3.

In the case of connection-less protocols such as IP the label techniques known as IPSO (IP Security Option) is used. Such labels (sensitive, unclassified, top-secret etc) are usually accompanied with encrypted data. If the data are sent to a trusty communication system (the delivery of data is guaranteed to be to a authorized local system) then the label could be satisfactory protection but in the case of untested network i.e a public data network then the packets of data are encrypted.

The placement of Authentication, Integrity and Confidentiality functions in the higher layers or directly in the Application Processes such is electronic mail is straight forward solution which is pragmatic but not optical. Placement of the security functions and mechanisms for each application (i.e for Virtual terminal, for File Transfer, for Directory services etc) separately requires excessive development and duplication of functionality. This approach also contradicts the principle that security should be an integral part of the whole communication system and services provided. However, the practice has shown that this approach is much more used today due to the complexity of the interconnected networks and different requirements for security in different applications.

The security functions and services in the networks are provided by employment of security mechanisms. The security mechanisms are also defined in the Open Framework [5]. They are briefly described in the chapter that follows.

4 Security mechanisms

Mechanisms and algorithms providing different security functions and services are all called security mechanisms. In fact these mechanism form a hierarchy:

Higher level mechanisms, such as security protocols and semantic message contents,

Lower level mechanism, such as cryptosystems, forming parts of the above mentioned higher level mechanisms,

Physical mechanisms, such as encryption chips and pieces of program code, implementing the above mentioned mechanisms.

The application of these mechanisms depend mainly on the security functions required and on the complexity of the system to be protected. The security of a local system can, to a great extent, can be ensured by physical security ar-

rangement. However, in a global open network it is impossible to guarantee security of communications by means of physical safeness and there cryptographic techniques are applied.

4.1 Cryptography

Cryptography is a long-established way to keep information secret but nowadays the cryptographic mechanisms are specially developed and used to protect transfer of data and information. There are many cryptographic mechanisms but as basic ones used in globally connected networks the following are considered: encryption and techniques for providing integrity and authentication of the messages. For more details see [8,9]

An encryption mechanism is used to convert a cleartext message into a cryptogram. An encryption mechanism is based on a public algorithm and at least one key whose value is randomly chosen from larger set. A symmetric cryptosystem has two functions i.e encrypt and decrypt. A message encrypted with key K can be only decrypted with the same key [10].

In asymmetric encryption mechanisms the key is divided into two parts, the encryption key and the decryption key, in such a way that the encryption key specifies the encryption transformation and the decryption key determines its left inverse mapping decryption. The receiver of data holds a secret key with which he can decifer but a different key is used by the sender to encipher and this can be made public without in any way compromising the system. This system provides secure communication in only one direction. It is known as asymmetric or public key encryption mechanism.

If it is unfeasible to derive the encryption key from the decryption key then the system is called public key signature mechanism. In that case additional information is required to check the digital signature. An asymmetric encryption mechanism provides complete confidentiality (only the legitimate recipient in possession of the secret key can decrypt the message) but no authentication of the sender (anybody with access to the recipient's public key could generate the message) but if the technique of digital signature is applied then authentication can be provided too. Unlike a normal signature on a document, the value of the message i.e the whole plaintext of the message is transformed. In order to check the signature, the receiver applies the encipherment function using the public key of the sender. If the result is a plaintext message, the signature is considered to be valid. The argument for its validity is that only by possessing the secret key could anyone produce the transformed message which enciphers with the public key to generate a valid plaintext. There are other ways of forming digital signature in which the signature is not transformation of the message itself but an additional and separate value that goes along with the plaintext. In that case also origin and integrity of the message may be claimed.

Data Integrity mechanisms provides means for the sequence of messages to stay intact. This means that no message have, undetected been omitted or duplicated and that the original ordering of the messages is preserved. Data integrity provides detection of the changes in the data being transferred, optionally recovering from the changes, when possible and reporting the cases where recovery is not possible. Usually the technique of a Checksum [11] or, preferable Cyclic Redundancy Check [12] is used to detect changes in the data stream. Both represent a special field in the message which content guarantee that the data were not changed.

Authentication is today used by use of passwords which are concerned as very vulnerable and that sort of Authentication is known as weak Authentication. Strong Authentication can be based on symmetric or public key cryptography. The procedure of Strong Authentication and key exchange is described in the CCITT Recommendation X.509 [13] or ISO 9594 [14]. With symmetric cryptosystems a mutually agreed pairwise key belonging to the appropriate security context is used for Strong Authentication between any pair of parties A and B. Public key signature mechanisms have several advantages over symmetric cryptosystems when used for authentication. Key management is greatly simplified by the fact that only public keys of the pairs need to be shared and only one key pair is needed for each party.

A rapidly growing area in that field is that of zero-knowledge techniques [15]. In these techniques, the secret authentication information of each party plays very much the same role as the secret key in the public key cryptographic system

but it can not be used for data encryption, only for data authentication and possible digital signature. Some existing zero-knowledge techniques make key management very simple by completely abolishing the need for user dependent public key. The draw back of these techniques is that they require the secret keys to be generated by a trusted third party and they can not be used for confidentiality.

In the case of cryptography, the physical mechanism at the bottom of the hierarchy that are needed to actually perform the cryptographic functions employed can be pieces of software running on a piece of hardware or hardware. With the transmission speeds offered by current data networks, the efficiency of the physical mechanisms used is becoming a major issue of system design. The choice between various physical mechanism is trade-off between economy, flexibility and performance. For details see [16].

4.2 Known cryptosystems

The most commonly used today cryptosystems are the Data Encryption Standard (DES) which development was initiated by US National Bureau of Standards but later resulted in many commercial applications [17]. The Rivest-Shamir-Adleman (RSA) algorithm is the most commonly used and probably most usable Public Key Cryptosystem today [18]. The Diffie-Hellman scheme first proposed as the first published "public key algorithm" is still concerned as one of the best methods for secretly sharing pairwise symmetric keys [19]. The algorithm is based on public "half-keys" and secret values associated with them. From their public half-keys the communicating parties can determine a pairwise session, which remains secret from other parties. This key can then be used for mutual authentication and or exchanging secret information.

5 Security policy

An integral part of the Open Security Framework is the Security Policy. A security policy is a set of rules which constrain one or more sets of security relevant activities of one or more sets of elements. Secure policy need not apply to all activities and elements in a communication system. This means that its specification must include a specification of the activities and the elements to which the policy applies. The rules for each security service are derived from the security policy.

Security policies are conventionally divided into Identity-Based and Rule-Based policies; Identity-Based security policies are based on privileges or capabilities given to users and/or Access Control Lists associated with data items and other resources. In a Rule-Based security policy, Security Classes are normally used for determining what is authorized behaviour. In identity-based systems, the users traditionally identifies himself by presenting to the system something he knows (e.g a password). This is often called "need to know" policy.

It is only after an explicit security policy has been stated that security becomes an engineering problem and every organization seriously interested in security should have one. The enforcement of the adopted security policy and monitory of security related events lies in the domain of engineering.

A body responsible for the implementation of a security policy is called Security Authority. Security Authority may be a composite entity but such entity must be always identifiable. A security domain is a set of elements under a given policy administered by a single authority for some specific security relevant activities. An activity involves one or more elements such as: connections between different layers in the protocol suite, operation relating to a specific management function, non-repudiation operations involving a notary etc. The enforcement of the adopted security policy usually goes through generation of security control information. One of them is a Security Label. A security label is a set of security attributes that is bound to an element, communication channel or data item. A security label also indicates, either explicitly or implicitly, the authority responsible for creating the binding and the security policy applicable to the use of the label. A security label can be used to support a combination of security services. Examples of security labels are: indication of sensitivity i.e unclassified, confidential etc, to indicate protection, disposal and other handling requirements.

Another very important Security Control Information (SCI) is the Certificate. A certificate con-

tains SCI relating to one or more security services. Certificates are issued by Certification Authority. It is used to convey SCI from an authority to entities which require this information to perform a security function. In general a certificate may contain SCI for all security functions.

The security mechanism described in the chapter above involve the exchange of SCI either between two communicating parties or between the security authority and the interacting parties. There are two common forms of protected security information that are used by the described mechanisms. One is called security token, used to protect security information that is passed between interacting parties. The other is called a security certificate, used to protect security information obtained from an authority for use by one or more of the interacting parties.

The Security Framework [5] does not define the methods and the procedures for implementing the Security Policy and related SCI. This is left to be developed by particular organization and system. The security models and techniques developed for VANs and globally interconnected networks is relatively new and the number of publicly known implementations is relatively small. The following chapter gives a brief overview of known applications in the field.

6 Applications providing secure functions in VANs

6.1 Kerberos

The most prominent strong authentication service in wide use today is the Kerberos Authentication Server created in the Athena project at MIT [20]. Kerberos is in everyday use in several major U.S universities and obviously has solved a number of security problems in them. In Kerberos, authentication is based on symmetric encryption which precludes the stronger service of non-repudiation and leads to the problems of key management. However, non-repudiation is not considered as a serious threat in university environment. Kerberos works in limited environments and therefore the number of shortcomings such as the possession of the all master keys by only one party i.e Kerberos itself can become unfeasible to be managed one day when the number of users and service grow.

6.2 Private Enhanced Mail

The other forthcoming application within the Internet is PEM (Private Enhanced Mail) [21]. PEM provides security services for e-mail users and is a result of the development efforts by BBN in Cambridge, U.S based on the RFC 1113-1115 which have been developed by IETF (Internet Engineering Task Force) Privacy and Security Research Group [22]. The services provided are the following: confidentiality, data origin authentication and connectionless integrity as defined by ISO [5]. These services are bundled into two groups:

1. default services meaning that all messages processed via PEM incorporate the authenticity, integrity and non-repudiation support facilities and

2. optional services such as confidentiality.

For compatibility purposes PEM is designed to be transparent for X.400 message transfer agent systems. In the recipient's workstation PEM messages may be retrieved also by Post Office Protocol [22] or by IPMS protocol P7 as defined in X.400 environment [23].

PEM message processing involves three steps: SMTP (Small Mail Transfer Protocol) canonicalization needed for compatibility with the MTAs, computation of the message integrity code (MIC) and computation of the optional message encryption code. The second step begins with the calculation of MIC (similarly to DES message authentication code) then encryption follows if required by the originator. Message key, used exclusively to encrypt the particular message, is generated specially for that message. The encryption algorithm employed is specified in the Key-info field in the PEM header along with any parameters required by the algorithm. The message text is then encrypted using this per-message key. The third and final processing step renders encrypted or MIC-only message into a printable form suitable for transmission via SMTP or other messaging systems.

To provide data origin authentication and message integrity, and to support non- repudiation with proof of origin, the MIC computed in step 2

is padded and then encrypted using private component of the originator's public public key pair. This effects a digital signature on the message, which can be verified by any PEM user. If the message is encrypted, this signature value is encrypted using the secret, per message key, which was employed to encrypt the message itself. The resulted value is 6-bit encoded and included in the MIC-Info field along with the identifiers of the MIC algorithm and digital signature algorithm. The MD2 hash function is employed as the MIC algorithm and the RSA algorithm is employed as the digital signature algorithm [22]. A hash function is a well defined function of a message which appears to generate a random number.

The PEM specification recommend use of public key cryptography for message integrity and authentication and for distribution of message encryption keys. PEM uses the public key certificates as defined in the CCITT X.509 Recommendation [13]. On the basis of X.509 definition of certificate handling an Internet Certification Hierarchical (ICA) scheme is envisaged in which different Certification Policy's are employed. ICA is expected to be developed in near future. For details see [21].

6.3 SecuDe System

SecuDE is software package which consists of Security Application Programmers Interfaces providing support for the application of the Authentication Scheme and Certificate Handling, The Privacy Enhanced Mail Support, X.400 Message handling and Key Management. The system provides various cryptographic mechanisms such as DES, RSA, hash functions, key generation and generation and verification of digital signature [24]. The signature algorithm employed is a composition of a hash function followed by an RSA function. The signer's public key which is used for the verification of the signature is certified by Certification Authority. For encryption, the DES algorithm is used and for the transfer itself the secret DES key is RSA encrypted. For every user, the pair of RSA keys used for encryption and decryption is different from the pair of RSA keys used for signature and verification. A special module is provided for support of the functions for the generation and distribution of keys, certificates and certification paths enabling the functionality of the Certification Authority as envisaged in X.509. Additional module is also developed for support of PEM and secure X.400 mail [25].

6.4 EDI and Inter-Bank payment system

Other applications of the Security Framework Services are in the EDI environment and in the Inter-Bank payment systems [26]. Some of them (i.e the system ETEBAC 5 developed in FRANCE [27] use the authentication mechanism as defined in X.509 and the C (Message Authentication Code) computed on plaintext data. MAC is defined in the document ANSI Financial Institution Message Authentication and is a sort of authenticator). The MAC key is exchanged (encrypted under RSA) for each session. The confidentiality is configured by another key drawn by the sender. The non repudiation is based on the RSA algorithm. The digital signature comprises the MAC calculated on the Message Identifier and MAC calculated on the whole message. The secret key of the sender issued for computation of the signature.

The Holland AMRO-ABN bank implementation comprises two modules: a one way hash function which compresses the bulk payment to a code of a fixed length. This module is based on the DES algorithm. The output code of the module 1 (hash function) is encrypted with an RSA digital signature to provide currently authenticity and non-repudiation . Three main functions are essential: user identification, generation of digital signature and verification of digital signature. The necessary key management is based on the generation of the keys by every user and the certification of the keys by a Certification Authority after checking both the integrity and authenticity of the keys. Key generation is planned to be based on CCITT X.509.The response messages are used to provide non-repudiation of receipt.

Teletrust (Trustworthy Telematic Transactions) implements the public key mechanism and reliable hashing functions. The basic Teletrust device is a token.It is a credit card size chip that can not be tampered. The token is protected by a PIN (Personal Identification Number, a sequence of digits used for identification of the holder of a bank card) and is used as payment device. The

token is activated by the user and the mutual authentication with the service provider is performed by exchange of the public keys with RSA. Once completed, a payment transaction may take place and the token is used to "sign" the payment (digital signature).The authentication requires a Certification Authority (in this case the central bank). The token stores therefore the public keys and the signatures of the central bank used for the authentication of the users's bank, which is used for authentication of the user and the user, which is used for the authentication of the transaction.The digital signature is used for authentication, integrity and non-repudiation service.

7 Conclusion

Security is a central consideration in the evolution of Value Added Networks. Security services and functions are needed to protect the infrastructure of the communication system, the local resources as well as to provide enough assurance to the prospective users by guaranteeing safe transport of sensitive and high value information. Fortunately, today the fast progress of technical developments is rapidly improving the security of the networks providing in the same time openness, connectivity and safety.

References

[1] R.Reardon (ed.) *Future Networks*, Blenheim Online, London 1989.

[2] *Internet: Getting started*, SRI International, Menlo Park, CA, 1992.

[3] J.B. Postel, (ed.) *IAB official protocol standards*, 1992 J.B. Postel, Internet Protocol, RFC 791, 1981.

[4] ISO, Information Processing Systems, *Open System Interconnection Reference Model, Part:1 Basic Reference Model*, ISO 7498-1, Geneva 1984.

[5] ISO, Information Processing Systems, *Open System Interconnection Reference Model, Part:1 Security Architecture*, ISO 7498-2, Geneva 1988.

[6] R.Grimm, *Security on Networks: Do WE Really Need it?*, Comp.Networks and ISDN Systems, Vol.17, No 4&5, October 1989, p.315–321.

[7] A.T.Karila, *Open System Security - an Architectural Framework*, Espoo 1991, Helsinki.

[8] D.W.Davies and W.L.Price, *Security for Computer Networks*, Sc.ed.,J.Willey and Sons, Chichester, 1989.

[9] S.Muftic, (ed.) *Security Mechanisms for Computer Networks*, Ellis Horwood Ltd, Chichester, 1989.

[10] C.Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, Vol.28, 1949, p.656–715.

[11] ISO, Information Technology, *Security Techniques, A Data Integrity Mechanism*, ISO DP 9797, Geneva 1990

[12] S.Walker, *Network security: The parts of the Sum*, Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy, Oakland 1989, p.2–9.

[13] *The Directory - Overview of Concepts, Models and Services*, CCITT Recommendation X.500, Melbourne 1988, and The Directory, Part 8: Authentication Framework, CCITT Recommendation X.509 (Melbourne 1989,).

[14] ISO 9594, Information Processing Systems, *OSI - The Directory*, 9594 through parts 1 - 8, Geneva 1989.

[15] ISO 10181, Information Technology, *OSI Security Model*, Part 1 Security Framework, Part 2, Authentication framework A.Shamir, Identity-Based Cryptosystem and Signature Scheme, Advances in Cryptology: Proceedings of Crypto 84, Springer, Berlin, 1985, pp.47–53.

[16] J.Smith, *Cryptographic Support in a Gigabit Network*, INET 92, Proceedings, Internet Society Reston VA, Kobe, 1992, p.229–239.

[17] R.M.Davis, *The Data Encryption Standard in perspective*, Computer Security and the Data Encryption Standard, National Bureau

of Standards Special Publication, 500-527, Washington, 1978.

[18] R.Rivest, A.Shamir, L.Adleman, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communication of the ACM, Vol.21, No.2, 1978, p.120–126.

[19] W.Diffie,M.Hellman, *New Directions in Cryptography*, IEEE, Transaction on Information Theory, Vol IT-22, No.6, 1976, p.644–654.

[20] D.Otway, O.Rees, *Efficient and Timely Mutual Authentication*, ACM Operating System Review, Vol 21, No.1, 1987, p.8–10.

[21] S.Kent, *An Overview of Internet Privacy Enhanced Mail*, INET 92, Proceedings, Internet Society Reston VA, Kobe, 1992, p.217–227.

[22] J.Linn, *Privacy Enhancement for Internet Electronic Mail*, Part III, Algorithms, SRI NIC International, RFC 1115, Auvgust 1989.

[23] M.Rose, *Post Office Protocol: Version 3*, SRI NIC International, RFC 1225, May 1991.

[24] R.Grimm, R.Nauster, W.Scheider, *SecuDE, Principles of Security Operations*, Technical Report, Version 2.0, GMD, Darmstadt, Germany, 1991.

[25] *Message Handling Systems*, Recommendation X.400, CCITT, Blue Book Vol VII, Fascicle VII.7, Melbourne 1988.

[26] B.Jerman-Blažič, *Security in Value Added Networks – security requirements for EDI*, Comp.Stands, North Holland, Vol.12, 1991, p.23–33.

[27] *The TEDIS Programme 1988-1989*, Activity Report, and TEDIS-EDI Security Workshop, Security in a Multi-Owner System, Brussels, June 20-21, 1989, Digital Signature in EDIFACT a TEDIS programme report prepared by CRYPTOMATHIC A/S, final version, Nov.29, 1990.