26

Data Protection in Communications and Storage

by

Per Kaijser
Siemens Nixdorf Informationssysteme AG
Otto-Hahn-Ring 6
D-81739 Munich
Germany

Abstract

This paper presents the different kinds of data protections that can be achieved by IT-technology in data communications and in the storage of data. Data integrity, data confidentiality, data origin authentication and a set of non-repudiation services are examined in detail on what is actually achieved depending on how and where the protections are made. These can be performed either on the data object itself or by the communications or storage systems. It is shown that certain types of protections, such as the non-repudiation services, depend on where they are made, whereas others are independent thereof.

1. INTRODUCTION

Communication and storage of data in electronic form is used more and more in our society. As a consequence, requirements for data protection are increasing, particularly for open systems with several interconnected networks [1-2]. Some data require protection against modifications, i.e. data integrity protection, and others may contain sensitive information requiring data confidentiality protection. Besides these two security services that are really protecting the data, this paper also deals with data origin authentication and a set of non-repudiation services. These are concerned with the trustworthy proofs of data and of actions associated with the data. Although these latter security services are not data protection in its true sense, they are directly associated with the data and thus included in this report. In the broad area of security in open systems, this paper is limited to the topic of data protections in communications and in storage, but excludes non-reversible data confidentiality protections that are commonly used in authentication protocols.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

There are several ways to protect data. These can be categorised according to the kind of protection they achieve, according to the mechanism involved or according to the component performing the protections, i.e. for what, how or where the protection is made. All these classification schemes are thoroughly described in Section 2. In the case of communications and storage of data, it is found that the scheme based on where the protection is made is particularly useful. Here the protection is either made by the storage or communications systems, or is physically connected to the data object itself forming a protected object. Such an object can then be securely communicated or stored independently of the security properties of those systems.

This paper describes all those different approaches in some detail. It is not the purpose of this paper to recommend a particular solution, but rather to show what protections are possible, what properties they have and how and where they are achieved. It shows that certain data protections, particularly those concerned with non-repudiation services, are strongly dependent on the entity performing the protection. Section 3 deals with data protections in communications and Section 4 those in storage.

Open systems rely on the existence of standards. Sections 3 and 4 include a brief description of some relevant international standards in existence and under development. The emphasis is on their applicability to the different approaches to data protection rather than their actual specifications.

A discussion including tables, that illustrate how the functional protections are related to the different protection schemes, is found in Section 5. It is hoped that these results will improve the communication between procurers and vendors of IT systems, since it will be easier to see what solutions best support the customer's security policy.

2. DATA PROTECTION METHODS

There are many ways in which one can classify the different forms of data protection. In this section three different classification schemes are described and examined. Section 2.1 describes the protections in terms of functionality as defined in ISO [1] and Section 2.2 makes in terms of the method used, i.e. how and where they are made. Finally, Section 2.3 contains an analysis of the relationships between these schemes.

2.1. Functional classification of data protection according to ISO

The conventional way of categorising data protection is by the functionality the security protections provide. Those relevant for data are:

- **data confidentiality**,
- **data integrity**,
- **data origin authentication**, and
- **non-repudiation services**.

In ISO [1], these are defined as:

Data confidentiality is defined as the property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Data integrity is defined as the property that data has not been altered or destroyed in an unauthorised manner.

Data origin authentication is defined as the corroboration that the source of the data received is as claimed.

Non-repudiation service is a security service to protect against repudiation, which is defined as the denial by one of the entities involved in a communication of having participated in all or part of the communication.

The first two are really protecting the data. The main purposes of the other two are quite different although they both provide data integrity as a side effect. Within each of these, there are different levels of protection, as will be seen in Section 2.3 below.

2.2. Technical classification of data protection

Data protection can be classified on the basis of the method used. The method has two aspects, the mechanism and the performing component or entity. The mechanism describes how the protection is made and the component where it is made. This subsection starts with the classification according to the mechanisms followed by that according to the components or entities.

Of the different technologies that mechanisms rely on, there is a need to distinguish between:

- **external data protection**,
- **transformation of data**, and
- **internal data protection**.

External data protection: The protection mechanism does not need to have access to the data. A typical example is access control, which has information about the data but does not need to know anything about the data itself.

Transformation of data objects: This is a protection based on cryptographic technology. The method requires access to the data object. There is no need to know anything more about the content of the data object than its string of bits. It transforms the data as a single atomic unit and creates some additional data, which contains information of how to make use of it. The original data object may be changed or left unchanged by the transformation. It can only remain unchanged in an integrity protection transformation. A transformation thus protects the whole data object without knowledge of its internal structure. Although cryptographically identical, there are reasons to distinguish between two variants depending on the handling of the additional pieces of information:

- **detached transformation**, and
- **attached transformation**.

In a **detached transformation**, the additional pieces of security information are kept separated (detached) from the transformed data. The additional pieces can e.g. be held in a special communication protocol field or in the directory of a storage system.

In an **attached transformation**, the transformed data and the additional pieces of security information are kept together forming a new object, a protected object. In this case the additional pieces are either encapsulating the whole original data object or attached to it.

Internal data protection: The protection here forms part of the data object itself. Only parts of the original data object can be protected and it is thus essential for the method not only to have access to the data, but also to understand its internal structure. The protection of the parts is by means of a transformation, often in the detached form with the detached pieces kept within the data object but separate from the protected parts [3].

It is recognised above, that the internal data protection and the attached transformation are mechanisms where the protections are physically connected to the data object themselves. This leads to the third classification scheme, namely according to the component or entity in the IT system performing the protection. In the case of communications, data protections can be made either by the communication system or on the data object itself. The same two modes of protection also apply to data in storage. There are thus two data protection classes according to the entity performing them:

- **by the communication or storage system**, and
- **on the data object itself.**

This classification has the advantage that it better clarifies the properties of and impacts on the components of the system. It thus gives procurers of IT-systems an excellent criteria for choosing a solution that best suits their security policy. This classification has been used in Sections 3 and 4 describing data protections in communications and in storage, respectively. The relationships between this classification scheme and the mechanism scheme will be further discussed in Section 5.

2.3. An analysis of the functional classifications in terms of methods

Below follows an analysis of the different protections according to the functional classification above (Section 2.1). The kinds of protection that they can achieve as well as their dependence of mechanisms and entities are examined in detail.

Data confidentiality: Two levels of data confidentiality are possible:

- to keep unauthorised users unaware of the existence of the protected data,
- to keep unauthorised users unaware of the semantic content of the protected data.

The former is achieved by means of access control [4], i.e. an external protection. It is thus limited to servers or applications holding the data.

The latter is achieved by enciphering the whole or parts the data object [3, 5], i.e. a transformation or an internal data protection. It is conventionally made by means of symmetric key technology, i.e. a cryptographic method where the key used to encipher the data is the same as that required to decipher the enciphered data. This key is called a 'secret key' since it has to be kept secret between the partners involved.

Data integrity: At least three kinds of data integrity are possible:

- to protect against modification of the data by unauthorised users,
- to detect a modification of protected data,
- to detect missing data in a sequential order of data.

Controlling that modification is not performed by unauthorised users is done by means of access control [4], i.e. external protection. It is thus, as for confidentiality, limited to servers or applications holding the data.

The detection of modification of data is the conventional mechanism for data integrity [6]. This protection neither protects against a modification nor does it restore the true content from modified data. It is made by a transformation or an internal protection and is usually achieved by letting a one way function (OWF), also called a hash function, act on the data making an additional piece of data, a 'fingerprint', of a certain well defined length. This new set of data should be long enough and the OWF have properties such that it shall be practically impossible to create another piece of data resulting in the same 'fingerprint'. The 'fingerprint' is then protected by some kind of cryptographic technology. This can either be achieved by a symmetric or an asymmetric algorithm. In the former case, the data is integrity sealed and in the latter it is signed. The asymmetric algorithm involves two keys, a private key to form the signature and known only by its owner, and a public key that is publicly available and used to verify the signature. These algorithms are therefore also often called public key algorithms.

There is also the possibility to keep track of the sequential order of data objects sent from a given sender to a particular recipient by a protected message numbering scheme or by references, e.g. to a previous message.

Data origin authentication: The data origin authentication serves the purpose of convincing the receiver or reader of the data about its source (origin). It is achieved by the same kind of cryptographic technology as to provide data integrity detection. Data integrity protection is thus part of data origin authentication. As will be seen later there are different types of sources (origins), such as creator/author, owner, or sender of the data. For documents and books one talks about three categories of origin, namely author, preparer and owner [7]. In many situations the proof of origin is limited to a claimed origin.

Non-repudiation: There are a set of non-repudiation services [8]. Their main purpose is to settle a dispute between two partners, normally two human users, by means of a proof that is able to convince a third party, e.g. that the data has been written (proof of creator/author, owner), sent (proof of sender, submission, delivery) and received (proof of receipt) by one of the partners. The different services are described in detail in Sections 3 and 4.

There are principally two modes of working. One involves a notary service which is trusted to have a correct recording of the matter. The other, and in IT-technology of more interest, is the use of a digital signature (see above). Only the signature scheme is treated further in this paper. Note, that data integrity is supported by all, and data origin authentication by some, of the non-repudiation services.

3. DATA PROTECTION IN COMMUNICATIONS

Data protection in communications can be achieved by two principally different approaches. One way is to let it be done by the communication system. Here the additional pieces of information from a detached transformation are appearing in the protocols associated with that communication. Alternatively, the protection can first be made on the data object itself and then later transferred by the communication system. In the latter case no information related to security is found in the protocols, with the possible exception that it might contain a statement of the type of data that it communicates.

The most common approach is to let the communications system provide the data protection service. There are some advantages with this approach. It implies that only those communication links requiring protection need to perform it. The overhead and computer time may thus be reduced. It can also be done at one of the lower layers of the communication stack according to the requirements for that particular link. It is normally computationally more efficient to make a transformation in a lower layer. On the other hand, the higher the layer of the protection, the closer to end-to-end protection and thus a better control over the security of the data.

However, these advantages also imply disadvantages. The protection is only over the protected communication links, which implies that the user or the system might need to control the routing of the data transfer. In some environments it might be enough to protect the wide area network (WAN) leaving the local area network (LAN) unprotected. The handling of sensitive data then needs to consider sensitivity and routing. This puts extra burden on the personnel or applications handling such data. The protection is furthermore normally at the lower layers, i.e. not an end-to-end protection. The X.400 Message Handling System [9] is one of the few communication systems, that offers a number of data protection services at the application layer, i.e. between sender and the mailbox of the recipient.

The main advantages of making the protection on the data object itself are the true end-to-end protection it provides, and that it is completely independent of the communications systems; it even provides secure communication on physical media such as floppy discs. The disadvantages are, that the user (or application) has to make the decision if and how the data shall be protected. It is not automatically supported by the infrastructure. This implies that the key distribution has to be handled by the same end-user that are handling the objects themselves.

The possible data protections that can be supported by communication systems are described in the next subsection followed by a subsection describing the possible protections that can be achieved when the protections are performed on the data object itself.

3.1. Data protection provided by communication systems

The ISO OSI seven layer model [1] permits security protections on most of its layers. They have, however, many things in common. All communications below the application layer are made without interaction with the end-user. The creation and distribution of required keys are from the user point of view done automatically. The protection by a communication system is between the same end points as the end points of the protocols associated with that layer. Below follows a description of the possible data protections that can be provided by a communication system:

Data confidentiality: A listener or attacker of the communications will not be able to deduce the semantic content of the data. It is achieved by enciphering the whole data object by means of a detached transformation. The protection is provided between the entities between which the communication system protocol carries the detached security information.

Data integrity: The receiving end of the communication system is able to detect if a modification of the data has taken place. It is achieved by sealing or signing the whole data object and possibly other pieces of information, a detached transformation. The protection is provided between the entities between which the communication system protocol carries the detached security information. The protection neither protects against a modification nor does

it restore the true content from received modified data. There is also the possibility to keep track of the sequential order of incoming data objects from a given sender and thus detect if some data are missing.

Data origin authentication: The data origin authentication serves the purpose of convincing the receiving end the source (origin) of the received data. Data integrity forms part of data origin authentication. The type of source (origin) that communication systems can provide a proof of is:

- Proof of sender, it provides the recipient with a convincing proof of the sender of the data.

Non-repudiation: There is a set of non-repudiation services that can be supported by communications systems. These are mainly aimed for application layer communications and the initiating and receiving individuals, but can also be used to dissolve disputes between the user of a service and the service provider. The different proofs that communication systems can provide are :

- Proof of sender, i.e. it protects the recipient from the sender denying that the data in question has been sent by that user. (Note that this is called proof of origin in some communication systems, e.g. X.400 [9].)
- Proof of submission, i.e. it protects the sender from someone disputing the sender has actually submitted the data to the communication system. This dispute is normally from the communication service provider, but can also be from someone who did not receive some expected data.
- Proof of delivery, i.e. it protects the sender and/or the service provider from somebody disputing that the data has been delivered to the correct destination. It does, however, not provide proof that it has been received by the intended recipient. In case of electronic mail, it provides proof that it has been delivered to the mailbox, not that it has been picked up from it.
- Proof of receipt, i.e. it protects the sender from the recipient denying ever having received the data. This can only be achieved by those communication systems from which the recipient has to explicitly fetch the data.

In the area of communication protocols, there exists a set of International Standards incorporating security. They are valid for the different layers in the ISO OSI seven layer model. At layer 1, the physical layer, ISO 9160 [10] applies, at layer 3 and 4, the network and transport layers ISO/IEC 11577 [11] and 10736 [12], respectively. At the application layer the X.400 Series of Recommendations [9] specify a set of security services, which also applies to the interchange of EDI (Electronic Data Interchange) messages by means of X.400.

3.2. Data protection provided on the data object itself

When the data protection is made on the data object itself, another set of security features are achieved. The advantages with this mode of data protection is that they provide true end-to-end protection, e.g. from one end-user to another one or between two applications. The protection is independent of the communication system and allows even protected communications on physical media such as floppy discs. The communication system transfers the protected objects transparently as any other unprotected object. It is also possible to protect parts of the data object. This cannot be achieved by a communication system, which is unaware of the internal structure of the data it carries and thus always treat a data object as a single atomic unit.

The data protections that can be achieved are:

Data confidentiality: A listener or attacker of the communications will not be able to deduce the semantic content of the data. It can protect the whole object or parts of the data object. The protection is end-to-end.

Data integrity: The receiver of the data is able to detect if a modification of the data has taken place. The protection neither protects against a modification nor does it restore the true content from received modified data. It can apply to the data object as a whole or to parts of it. It should be noted, that it is not possible for a recipient to detect if the protected parts (whole or parts of the data object) has been replaced and the seal or signature has been deleted or replaced by an authorised user [3, 7].

The sequential order of data can in theory be achieved by explicitly numbering each object or by referring to the previous data object. It relies on the trust in the individuals or applications to correctly handle it; it is not an IT security service.

Data origin authentication: The receiver of the data is convinced who the originator of the data is. The originator is either the creator/author, preparer or the owner, but not the sender, of the data. It can be applied to the whole data object or parts of it. The same remark made for integrity above also applies.

Non-repudiation: There are essentially only two non-repudiation services that can be supported by this mode of communication protection. These are completely different from those provided by communication services. They are thus complementary to those. It can be applied to the whole data object or to parts of it. The proofs that can be provided by object protections are :

- Proof of origin, i.e. it protects the recipient from the originator denying that the data in question originates from that user. The originator is the creator/author, preparer or owner, but not the sender, of the data.
- Proof of receipt, i.e. it protects the originator or sender from the recipient denying having received the data. The creation of the proof is in this mode made explicitly by the recipient and normally only after a request from the originator or sender.

The International Standards in this area are limited. There is really only one International Standard today supporting these features, and that is the ISO 8613 or the CCITT (ITU) T.400 Series of Recommendations [7]. It provides protections of parts of a document conforming to the ODA standard. Although the standard only specifies how to protect an ODA document, the scheme can easily be generalised to protect any data structure fulfilling certain criteria [3]. There is presently no International Standard specifying how to protect a whole data object as a single atomic unit. There is a need for the specification of such a standard providing an envelope or attachment to the data structure.

4. DATA PROTECTION IN STORAGE

For the protection of data in storage there are also two principally different approaches. When data are stored in a file or similar storage system one can either let the storage system perform the protection, mainly in the form of access control, but also by means of information available in its directory, or by explicitly protecting the data objects themselves. The access control can either be done by the infrastructure, which controls the access to the storage

system, or by the storage system itself, which can control the access rights on each individually stored data object.

The conventional way of protecting data in storage is by means of access control. It has the advantage that it does not require any additional security features than already available in most systems. The additional protection of the data objects themselves is mainly done since the data are sensitive (from either the confidentiality or the integrity point of view) and that the access control is not fully trusted for the required protection. Another case is when the data is stored on physical media which might get into the wrong hands, e.g. by theft. Then, the protection of the objects themselves are the only means of data protection. This is also true, when parts of an object shall be protected.

4.1. Data protection provided by the storage system

A storage system is able to protect its data by means of access control. It can ensure that the right to read or the right to modify data is limited to users authorised to do so. It is, however, not possible to forbid an authorised user to modify data supposed to remain unchanged. An access control system is thus more concerned with the property of the user, i.e. if authorised or not, than with the actual data itself.

In addition to access control, a storage system is also able to keep pieces of security information in its internal directory. Examples are an integrity seal of the data and statements about the creator, preparer and owner of the data. The protection is valid against users that are not authorised to modify information in the directory associated with those objects.

The limitations of all these methods lies in the trust of the authorised users to only perform those actions that they are supposed to do. The kinds of data protection possible by a storage system are:

Data confidentiality: Two levels of confidentiality protection are possible, namely
- to protect against revealing the semantic content of the data to unauthorised users,
- to protect against revealing the existence of the data to unauthorised users.

These are both provided by access control systems. In the former case the accessor has access to the directory of the system but not the right to read the protected object. In the latter case the accessor can only see the entrances in the directory corresponding to objects which he (she) is allowed to read.

Data integrity: Again two levels of data integrity are possible, namely
- to detect a modification of the data by an unauthorised user,
- to protect an unauthorised user from modifying the data.

The former is possible by comparing the data object with the corresponding seal or signature in the directory of the system (detached transformation). The latter is made by means of access control. It is noteworthy, that within the scope of this paper, this is the only method and environment that actually protects against modifications.

Data origin authentication: The storage system can provide the accessor of the data with a proof of origin of the data. The origin is the owner of the data, which can be either the one who stored it or the storage system itself. For data that is publicly accessible, the data origin authentication shall be done by a digital signature so that any reader can verify its origin and

detect any modifications. These kinds of information is found in the directory of the storage system.

Non-repudiation: There is less need for non-repudiation services for storage systems then for communications, but for publicly accessible data it is quite useful. A digital signature in the directory of the storage system can be used for:

- Proof of origin, i.e. it protects the accessor (reader) from the originator denying being the owner of that data. Either the one who stored the data or the storage system itself can be the owner of the data.

Most protections of data in storage systems are relying on access control. In the International Standardisation arena, ISO/IEC JTC1 presently develops a standard for the production and distribution of access rights in distributed systems. It is based on the work of ECMA, SESAME and the Distributed Computing Environment from Open Software Foundation (OSF DCE). SESAME is a project of Bull, ICL and Siemens Nixdorf [13, 14] that is sponsored by the European Commission. OSF DCE is based on Kerberos from MIT [15] and SESAME on the works of ECMA (European Computer Manufacturers Association) [2, 16 - 18].

4.2. Data protection provided on the data object itself

When the data protection is made on the data object itself, essentially the same set of data protections are possible as for the communication of such data (Section 3.2 above). An important observation is that all protections can be applied to either the whole object or to parts of it. They do furthermore also protect data stored on removable physical media, such as those used in certain back up systems. The possible data protections are:

Data confidentiality: It is not enough for the accessor (reader) to have physical access to the data, in order to get semantic knowledge of its content. He (she) must also be able to decipher it. This technique is quite useful for the protection of sensitive parts of an object.

Data integrity: The accessor (reader) of the data is able to detect if a modification of the data has taken place. The protection neither protects against a modification nor does it restore the true content from modified data. The same limitation on data integrity exists as described in Section 3.2 above.

Data origin authentication: The accessor (reader) of the data can be convinced who the originator of the data is. The originator is in this case not only the owner, but can also be the creator/author or preparer of the data. The owner is, however, limited to the one who stored it; it does not include the storage system as in the previous section. As above, a digital signature is particularly useful for publicly available data.

Non-repudiation: A digitally signed data object can be used for the same type of non-repudiation service as when performed by a storage system, although with a slightly different scope of origin, namely

- Proof of origin, i.e. it protects the accessor (reader) from the originator denying that the data in question originates from him/her. The originator is, as for data origin authentication, either the creator/author, preparer or the owner of the data.

Since the ODA standard [7] and its generalisation [3] describe data structures, they apply to both the storage of a document or a data structure as well as to its communication. The text at the end of Section 3.2 related to standards is thus equally valid for this section.

5. DISCUSSION

The previous sections have shown that data protections can be achieved by different methods and that depending on where and how the protections are made, there are principle differences between the kinds of protection achieved. Table 1 shows a summary of the classifications of the methods. It is in the form of a matrix with two rows and four columns. The first row represents the case when a component of the communications of storage system performs the protection, and the other when the protection is made on the data object itself. The four columns stands for the different mechanisms described in Section 2. The entries specify whether the method protects the whole data object, 'W', or parts of an object, 'P'.

Table 1
Summary of data protection methods

Protection by component or on the object itself	Mechanism			
	External	Transformation		Internal
		Detached	Attached	
Communications or storage system	W	W		
Object			W	P

From the mechanisms, one recalls that a transformation has two variants. Although cryptographically identical, they belong to different rows in the table. There is thus a fundamental difference in the semantics between these two transformations, as will be seen below, that cannot be deduced from a pure cryptographic point of view. From the second row of the matrix, one also observes that the internal protection can be seen as a special case of the attached transformation, namely a protection with a finer granularity.

The results of Sections 3 and 4 are summarised in Tables 2 and 3, respectively. Table 2 contains the true data protections, i.e. data confidentiality and data integrity, and Table 3 the data related protections, i.e. data origin authentication and the non-repudiation services.

For data confidentiality, it is found that either the system component scheme or protection on the data object itself can be used for the most conventional objective, namely keeping the semantic knowledge of the content of the whole data object unknown to unauthorised users. By means of object protections, additional features can be obtained, such as protections of data on physical media and of parts of an object.

Table 2
Summary of methods for data confidentiality and data integrity

Data protection	Communications			Storage			
	System	Object		System		Object	
	Detached transf.	Attached transf.	Internal	External	Detached transf.	Attached transf.	Internal
Data confidentiality							
Knowledge of existence				W			
Sem. knowledge of content	W	W	P	W	W	W	P
Sem. knowledge of content on physical media		W	P			W	P
Data integrity							
Control of modification				W			
Detection of modification	W	W	P		W	W	P
Detection of modification on physical media		W	P			W	P
Sequential order	W	(W)					

Table 3
Summary of methods for data origin authentication and non-repudiation services

Data protection	Communications			Storage			
	System	Object		System		Object	
	Detached transf.	Attached transf.	Internal	External	Detached transf.	Attached transf.	Internal
Data origin authentication							
of creator/author/preparer		W	P			W	P
of owner		W	P		W	W	P
of sender	W						
Non-repudiation of							
creator/author/preparer		W	P			W	P
owner		W	P		W	W	P
sender	W						
submission	W						
delivery	W						
receipt	(W)	W	P				

For data integrity, it is found that the conventional protection is not what the user would prefer, namely protection against modifications, but an indirect solution to detect if a modification has taken place. This is of course due to the impossibility to provide the former other than by means of access control, which is limited to a storage system, such as a file server. The detection of a modification of a whole data object is possible by both the system

component and the data object protection schemes. Additional features can, as for data confidentiality, be achieved by the object protection method.

The bracket around the protection of sequential order indicates that it is not an IT service, but rather something that the user can enter in the content of the object. The protection is thus possible in principle, but relies on a combination of a non-technical and a technical mechanism, the latter in the form of detection of a modification (data integrity).

Data confidentiality and data integrity can thus be achieved by either the service component or on the data object itself. If one momentarily excludes the protection of parts of a data object, there are advantages and disadvantages with the different approaches. Advantages with protection of the data object itself are the independence of communication and storage systems, and that it provides true end-to-end protection. If for example several communication systems are to be supported, they all ought to support the same security policy. By protecting the objects themselves, none, rather then all of them, need to incorporate the often expensive security features. It is also the only means of securely protect data on physical media such as floppy discs and back up systems. Disadvantages are that the cryptographic keys must be controlled by the applications or the users involved. It puts a higher burden on users and applications. If not handled in a well organised manner, there is the danger of permanently loosing enciphered data on a storage system or storage media.

If there is a requirement to protect data on a physical media or to protect parts of a data object, then the protection has to be provided on the data object itself.

For data origin authentication and for non-repudiation services the protections differ quite substantially depending on the method, and particularly with respect to where the protection has been made. It turns out that the services provided by the communication and storage systems are complementary to those performed on the object itself. Certain user communities may require both approaches in order to provide the relevant proofs. This is clearly visible in Table 3, where the services are summarised.

Some proofs for non-repudiation might for legal reasons need to be accessible for a long period of time. For such cases, it is probably better to have the proofs directly attached to the data itself. But as seen in this report, only a limited set of proofs can be achieved on a protected object.

The bracket in the table for non-repudiation of receipt indicates that it is only possible for a limited set of communication systems as described in Section 3.

A procurer of an IT-system providing data protection need to analyse the requirements carefully. Factors like the time period over which the data must be protected, the ability to control the routing by communications, the back up system and similar issues need to be considered together with the security policy. It is only after a combination of such an analysis and an associated threat analysis, that the required data protections can be specified and a decision made if no, one or more protection methods need to be supported. In particular, it is important to know, which entities should be capable of providing data security. Note, that the non-repudiation services, which are expected to have legal impacts on business agreements, might need to be implemented on both the communication system components as well as on the entities or components performing protections on the data objects themselves.

In conclusion, it is found that for the true data object protections, there is a choice of which component or entity that shall perform the protection. The exception is if protections on physical media such as floppy discs and of parts of a data object are required. For data origin authentication and the non-repudiation services there is, on the other hand, really no choice, it is rather a matter of the particular services that the policy requires.

REFERENCES

1. ISO/IEC 7492-2 "Information Technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture" (1989).

2. ECMA TR/46 "Security in Open Systems - A security framework" (1988).

3. P. Kaijser, "Security protection for parts of a data structure" Comput. Commun., Vol 17 No 7 (July 1994) 476.

4. ISO/IEC 10181-3 "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 3: Access Control" (in preparation).

5. ISO/IEC 10181-5 "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 5: Confidentiality" (in preparation).

6. ISO/IEC 10181-6 "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 6: Integrity" (in preparation).

7. ISO 8613 "Information Processing - Text and Office Systems - Open Document Architecture (ODA) and interchange format", (also published as the ITU (CCITT) T.400 Series of Recommendations) (1989).

8. ISO/IEC 10181-4 "Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Part 4: Non-repudiation" (in preparation).

9. CCITT (ITU) X.400 Series of Recommendations "Message Handling System", (also published as ISO/IEC 10021, Message-Oriented Text Interchange Systems (MOTIS)) (1988).

10. ISO 9160 "Information Processing - Data Encipherment - Physical Layer Interoperability Requirement" (1988).

11. ISO/IEC 11577 "Information Technology - Telecommunications and Information Exchange between Systems - Network Layer Security Protocol" (1994).

12. ISO/IEC 10736 "Information Technology - Telecommunications and Information Exchange between Systems - Transport Layer Security Protocol" (1994).

13. T.A. Parker, "A Secure European System for Applications in a Multivendor Environment (The SESAME project)", Proc. 14th Am. Nat. Security Conf., Washington, DC (1991).

14. P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The solution to security for open distributed systems", Comput. Commun., Vol 17 No 7 (July 1994) 501.

15. J.G. Steiner, C. Neuman, and J.I. Schiller, "Kerberos: an authentication service for open network systems" USENIX Winter Conf., Dallas, TX (1988) 191.

16. ECMA-138 "Security in Open Systems - Data Elements and Service Definitions" (1989).

17. ECMA-206 "Security in Open Systems - Association Context Management - including security context management" (1993).

18. ECMA-219 "Security in Open Systems - Authentication and Privilege Attribute Security Application with related Key Distribution Functions" (1994).