

/

Project P514

CCS#7 Networks Dependability Studies: Phase 2

Deliverable 2

CCS#7 network integrity aspects and qualification techniques - Access control

Volume 2 of 3: Annex A - Protocol analysis in Access Control

Suggested Readers:

Departments in charge of specifying, planning, installing, testing and maintaining CCS#7.

For full publication

June1998

EURESCOM PARTICIPANTS in Project P514 phase 2 are:

- France Télécom
- TELECOM ITALIA S.p.a.
- Hellenic Telecommunications Organisation S.A. (OTE)
- Telefónica S.A.
- MATÁV Hungarian Telecommunications Company Ltd.

This document contains material which is the copyright of certain EURESCOM PARTICIPANTS, and may not be reproduced or copied without permission.

All PARTICIPANTS have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the PARTICIPANTS nor EURESCOM warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

This document has been approved by EURESCOM Board of Governors for distribution to all EURESCOM Shareholders.

Preface

(prepared by the EURESCOM Permanent Staff)

EURESCOM Project P307 tried to make an analysis of the most common problems caused by faults in the CCS#7 networks. Due to the lack of information, because PNOs consider this information very sensitive and secret, they could not produce good results.

Having this experience in mind, EURESCOM Project P514 was launched aimed at studying specific aspects of great relevance for CCS#7 network dependability and at defining verification methods and criteria to improve network integrity, without involving restricted information.

Project P514 was divided into two phases.

Phase 1 has collected information about network threats, protocols in use, network architectures, congestion control procedures in use, routing options and services implemented. The information that has been collected has pointed out three main topics related to the subject of network dependability. These topics are: access control, congestion control and automatic recovery of signalling links.

Phase 2 has made the real dependability studies. For each topic the Project team has done a theoretical analysis on the protocols used and the existing recommendations. Starting from this analysis test suites have been produced to check the integrity of the network for each of these topics.

This Deliverable refers to the topic of access control. The other two topics are described in D3 and D4. A last Deliverable, D5, will include a summary of all the facts.

Phase 1 ran for one year, while Phase 2 has been running for 27 months. The Project Leader during Phase 1 was Wilhelm Klein from DT who was replaced in Phase 2 by Ezio Paglieri from CSELT.

List of Authors

Fulvio ONEGLIA

IT

CSELT

Thierry BARITAUD

FT

CNET

Table of Contents

Preface.....	i
List of Authors.....	iii
Table of Contents	iv
1 Introduction.....	1
2 Identification of threats.....	3
2.1 Overview of network security threats.....	4
2.2 Security objectives for the CCS#7	5
2.3 Definition of a template for the threats analysis	6
2.4 Threats related to loss of integrity or corruption of signalling related data	7
2.4.1 Description	7
2.4.2 Types of information threatened	7
2.4.3 Point of attack and originator of the attack	7
2.4.4 Risks due to contamination of information	7
2.5 Threats related to masquerade and unauthorised access to resources.....	9
2.5.1 Description	9
2.5.2 Types of information threatened	9
2.5.3 Point of attack and originator of the threat.....	9
2.5.4 Risks due to masquerading as another entity.....	9
2.6 Threats related to eavesdropping or disclosure of information.....	10
2.6.1 Description	10
2.6.2 Types of information threatened	10
2.6.3 Point of attack and originator of the attack	11
2.6.4 Risks due to disclosure of information.....	11
2.7 Identification of the most sensitive access points	12
3 Protocol analysis.....	15
3.1 MTP.....	15
3.1.1 User part messages	16
3.1.2 Management messages	16
3.1.3 Parameters	18
3.2 SCCP	20
3.2.1 Upper level messages	21
3.2.2 Management messages	21
3.2.3 Parameters	22
4 Integrity mechanisms for the CCS#7 system.....	25
4.1 Overview of integrity services.....	25
4.2 Integrity mechanisms.....	26
4.2.1 Integrity provision through encipherment (for transmitted data).....	27
4.2.2 Integrity provision through MACs and MDCs (for transmitted data)	28
4.2.3 Integrity provision through digital signature	30
4.2.4 Integrity of stored data.....	31

5	Mechanisms to avoid unauthorised use of resources	33
5.1	Monitoring of signalling traffic	33
5.2	Screening of messages	33
5.3	Policing of activities	34
5.4	Where to adopt protection mechanisms	35
	References	37

1 Introduction

The purpose of the study on Access Control is to investigate the protection of the signalling system against the logical attacks that are activated intentionally or accidentally.

However, the analysis will not take into account physical threats like earthquake threat or physical destruction of signalling equipment by the sledge hammer strokes of a crazy man... The physical security may consist of a set of physical artefacts added to the system or to the system's environment. This type of protection technique protects the equipment or connecting lines of the signalling system from attacks via their physical surroundings. These physical measures may include door locks for rooms, tamperproof devices for key storage... Their investigation is out of the scope of this Annex.

The investigation of fraud whose goal is to fraudulently and freely take advantage of the network is also out of the scope of this Annex. These fraud related threats are service dependant and they are usually investigated for each specific service or network. The frequency of such threats is very high. They are sometimes very easy to implement, and an attacker may quickly and easily save or get money. These threats may generate huge losses of revenue but they "only" represent commercial losses. They do not endanger the vital functions and equipment of the backbone network.

The second chapter of this Annex deals with the identification of intentional and accidental threats leading to possible critical scenarios for the maintenance of the integrity and availability of the network. The difficulty to carry out the attacks and the likelihood of occurrence of the accidental threats is estimated and the risks and possible damage to the network is then evaluated. Finally, access points for an attacker and originating points for the accidental threats are identified.

The third chapter of this Annex reflects a deep CCS#7 protocol analysis. From this protocol analysis, signalling messages carrying sensitive information are identified. Then we investigate the consequences of misuse of these messages on the integrity and availability of the whole network, and the potential dangers for the network. Parameters and information to be checked before accepting a signalling message are then examined.

In this CCS#7 protocol analysis, some of the examples of the potential dangers for the CCS#7 are:

- Isolation of a specific node in the network.
- Congestion.
- Routing reconfiguration.
- Traffic diversion.
- Isolation of a user part.
- Sending of signalling traffic to non available MTP or STP.
- Prohibition and inability for an SCCP user to offer a particular service.
- Modification of the status of a remote subsystem.

Finally, in the fourth chapter, this Annex proposes possible solutions for the improvement of the protection of the current network and for the protection of the

network when opening new access points. These possible solutions mainly consist of adequate cryptographic mechanisms for protecting the integrity of the signalling network, and for preventing unauthorised access to the signalling network.

2 Identification of threats

Nowadays, open telecommunication networks are more and more interconnected. The possibilities to have access to a specific network are then more and more increasing. On the other hand, the possibilities for an attacker to get fraudulent access to a network or the possibilities for an entity to accidentally get access to a network for which it has not requested the access, are also increasing.

The purpose of any security policy is then to counter both intra-network related threats and inter-network related threats. In the telecommunication field, it is now commonly agreed that the accidental or intentional threats endangering a specific network are not only a matter for individual networks, but are recognised as a matter for all interconnected networks.

The purpose of this chapter is to analyse all the threats that endanger the integrity and the availability of the signalling network, whether these threats are accidental threats or intentional threats.

The objective of intentional attacks is to logically destroy or to inhibit some of or all the equipment of the signalling network in order to seriously degrade the efficiency, the integrity and the availability of the telecommunication network.

These intentional attacks on the integrity of the signalling system are more sophisticated than classic (confidentiality based, authentication based, ...) attacks or fraud on specific telecommunication services or on mobile telecommunication networks. Their likelihood of occurrence is also much lower.

However, these attacks on the signalling system are really sabotage related. If an attacker really wants to perform such an attack, it is because he can really benefit from it, or because he is really willing to block all telecommunication activities in this network.

The damage caused to this network by these attacks and the potential consequences of the loss of subscriber confidence in this operator and of the loss of revenue for the operator, may be critical for the victimised operator, because they endanger the vital functions of the operator.

In this chapter, we also investigate accidental threats whose likelihood of occurrence is much higher than those of intentional attacks. Even if the prevention of these accidental threats is not security relevant but safety relevant, the definition of counter-measures for such accidentals threats is of high importance for the availability of the whole network.

Figure 2.1 may be considered as a guideline to understand the way the threats analysis and the risks evaluation has been performed for the CCS#7.

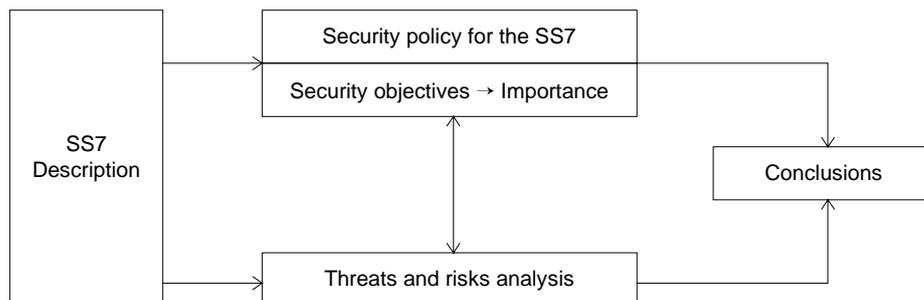


Figure 2.1 - Method to identify threats and associated risks for the CCS#7 network

2.1 Overview of network security threats

The threats jeopardising the availability and integrity of telecommunication networks depend of course on the type of the considered network. It is clear, for instance, that some of the threats identified for a private digital cellular mobile telecommunication network are quite different from the threats to a public signalling network.

However, some threats are common to all telecommunication networks. These common threats to security of telecommunications, are either malicious or unintentional, and may include the following examples:

- *Unauthorised use of, misuse of, or denial of access to, information or resources*
- *Modification of data and loss of integrity.* This includes:
 - removing or changing intended information;
 - adding wrong information;
- *Delayed transmission and replay of transmission*
- *Misdirected information*
- *Denial of service.* This can be achieved by:
 - prevention of others from performing their authorised functions by overloading network systems
 - flooding the network systems with requests and demands
- *Disclosure of information.* This means for example:
 - eavesdropping
 - traffic analysis (type, volume, timing, source and destination)
- *Feature interaction conflicts*
- *Fraud*
- *Denial of accountability* (by the sender or the recipient)

2.2 Security objectives for the CCS#7

Before investigating security measures to be added to network protocols, an analysis of the threats to the security of this network should be carried out. Only after a clear understanding of what type of threats a network must be protected against, can adequate security measures be designed and implemented.

It is necessary to consider the system context and the security objectives for the CCS#7 in order to be able to determine what type of actions may be considered as a threat to the security of the CCS#7 network and during what network operations such threats may arise.

The security objectives and security requirements for the CCS#7 are considered as follows:

- *high availability of the system*: for telecommunication operators, the maintenance of the accessibility and availability of the CCS#7 upon demand by an authorised entity is the primary security requirement of CCS#7 systems. Acceptable delay in obtaining authorised access to information or resources must be granted;
- *integrity of data and system*: one of the major security requirements for the CCS#7 is to have the assurance that the signalling related data have not been altered or destroyed in an unauthorised manner in the process of communication or while being stored. Modification of data in any unauthorised way endangers the reliability and the availability of the whole network;
- *setting up of different levels of rights of use and limitations of facilities offered*: entities within the network or within another network may be authorised to have different access rights to specific equipment or software, or may be offered different facilities by a telecommunication operator. This telecommunication operator may then want to restrict or enhance the right of use of certain specific entities, by providing these entities with corresponding access rights and set of facilities offered;
- *confidentiality of sensitive information*: It may be of crucial importance for a telecommunication operator to protect sensitive information related to charging and billing information, or to the structure of its network, the management of its equipment, or the profile of its subscribers. The maintenance of the confidentiality and the unavailability of this information to unauthorised individuals, entities or processes, is one of the main security objectives for the CCS#7.

These security objectives are the basis for the identification of the list of threats to the security of the CCS#7. Hence, based on the rating of the security objectives for the CCS#7 system, it is obvious that the most critical threats belong to the following classes of threat:

- threats related to loss of integrity of signalling data and resources;
- threats related to masquerading and unauthorised access;
- threats related to eavesdropping and disclosure of sensitive information;

The risks of all these intentional or accidental threats, including corruption, destruction, disclosure, loss or removal of resources, are the misuse of data or resources.

This Annex will focus on these identified classes of threat, and will only partly consider the threats (if they exist) belonging to other classes like denial of service-related classes, as they might be considered out of the scope of our study.

In this section, we do not cover the threats that are not directly CCS#7 related, like the non deletion when it is no longer required, of information copied into another network for the provision of an agreed service to a visiting user.

2.3 Definition of a template for the threats analysis

Taking into account these security objectives, the threats analysis can then be performed. It consists of a description of each identified threat including, as far as possible, the following information:

- *short description*: this includes a short plain text for a brief explanation of what this threat is supposed to do when it occurs.
- *types of information threatened*: this may be signalling data, control data or management data exchanged or stored in nodes, but there may also be other types like the statistics of traffic flow.

Signalling data may include sensitive address information and may also include cryptographic keys. Management data may include sensitive information about billing, security and information concerning the availability of the system, among other things.

- *point of attack*: this refers to a functional component or a reference point in the functional architecture, or to a physical point in the infrastructure.
- *originator of the threat*: this refers to the person, functional entity, physical machine in the network or within an external network, who/which performs the attack or who/which is the starting point (i.e. the initiator) of this threat.
- *risk due to the threat*: this risk is the result of a compromise after weighing up the following items:
 - profit for the attacker or for the entity from which the threat is coming: this includes the benefit (financial, economical or other) that the attacker or the originating entity can expect from this attack. This profit may be immediate or not.
 - damage caused by a successful attack: this is a very important indicator for the level of protection which is needed. It is clear that the damage to a network operator is not limited to the damage done directly in attacks which are actually carried out.
 - even greater damage (also economical damage) may be done if the users and subscribers lose confidence in the reliability, availability and security of the network operators and the provision of services. This loss of confidence may unfortunately be caused by the disclosure to subscribers and users of a few successful attacks, or even simply by a widespread belief that such attacks are feasible.
 - difficulty of the attack: the definition of the level of difficulty of the attack is of course under the assumption that no countermeasures whatsoever are already being provided.

This evaluation is based on assumptions about the knowledge, the means, or the financial support that an attacker needs. It may also result in the evaluation of the likelihood of occurrence of such a threat.

2.4 Threats related to loss of integrity or corruption of signalling related data

2.4.1 Description

Integrity of data means that the data have not been altered or destroyed in an unauthorised manner in the process of communication or while being stored. It may not always be possible to prevent attempts to alter or destroy the data.

However, in many cases in the protection of the CCS#7, it suffices to require that such alteration or destruction of signalling data will be detected and, if possible, corrected.

2.4.2 Types of information threatened

It must be pointed out here that it is not sufficient to protect only the integrity of individual CCS#7 messages. The complete set of signalling operations that must necessarily be performed in order to communicate successfully between two entities must be covered.

Threats to integrity can also arise from the duplication of signalling messages or a change in the order of the messages in a communication process which can lead to a disruption of this communication process.

If a very low error probability is required, standard error-correcting or error-detecting codes may not be sufficient.

However, both accidental and intentional alterations of the transmitted or stored information can be detected by adequate cryptographic measures with a very high probability.

But, the avoidance of modification of that data is much more difficult than its detection. It does not only require specific detection techniques for loss of integrity, but it also requires the use of access control or confidentiality techniques.

2.4.3 Point of attack and originator of the attack

The intrusion of an attacker in the fixed network may be difficult to realise, but is by no means impossible for a dedicated intruder.

The identification of the most sensitive access points is one of the key points before any efficient security policy is implemented.

2.4.4 Risks due to contamination of information

The loss of integrity of signalling data is considered to be the most risky threat to the CCS#7. It results in very critical scenarios for a network operator.

For example, threats related to the corruption of other network data, even if accidentally or intentionally initiated, could, for example, result in denial of service to a user because the user profile or subscription related data is no longer valid/readable.

Similarly, changing information which would then enable services to be used fraudulently is considered to be very risky for the operator. Indeed, the alteration of charging information may provide free use of services for a specific user or subscriber (e.g. for the fraudster).

Accidental threats: in case of accidental modification of data by an entity, the profit for the originator entity is not straightforward. If the data is changed in a nonsense message or information, the profit for the receiving entity is usually nil, or at least the consequences of this modification may cause some damage (delay, replay of message, downloading of information, additional processing...).

Of course, this profit may be high if the modified data is then changed into a profitable one, but as it has not been done intentionally, the receiving entity must also, in order to get some profit from the loss of integrity, accidentally benefit from it, or take the opportunity of this accidental modification to fraudulently take advantage of it. Hence, the profit for the receiving entity of an accidental loss of integrity seems to be very low.

But, the damage caused by this accidental modification of data may be very crucial and severe. Actually, accidental modification of data may result in the modification, contamination or destruction of information stored in databases like user profiles, subscriber identities, charging information related data.

This may also result in the changing of sensitive signalling messages to other understandable messages (replay or messages, delay in transmission of signalling messages, wrong routing of messages, replacement of sensitive messages by other messages...) disturbing the functionalities and the capacities of the whole network, creating congestion of links and equipment...

Intentional threats: in the case of an intentional attack, the profit for the attacker is generally the ability to get free access to a service or network, or more rarely to jam a network, to cause denial of services to specific users, or to sabotage the whole network.

The damage for the operator is then mainly loss of revenue. However, when the attacker is really trying to sabotage the functionalities of a network or trying to engender within the subscribers a loss of confidence in the reliability and availability of the network, the damage is either straightforward (congestion, isolation of an equipment, ...) or not (economical losses due to loss of subscribers...) and is much more important to an operator than the immediate loss of money due to a fraudulent action carried out intentionally by an individual attacker (person or machine) to get free facilities.

The high potential damage that may be caused by accidental or intentional loss of integrity of sensitive information is the main reason for the implementation of adequate countermeasures in the CCS#7.

The integrity services to be implemented as adequate countermeasures against integrity threats are only useful if the communicating parties are authenticated. The authentication can be used for providing security parameters and the required keys in order to obtain a secure CCS#7 channel.

2.5 Threats related to masquerade and unauthorised access to resources

2.5.1 Description

Before having access to a network, or a specific machine in this network, an entity must identify itself, and the network protection mechanism then authenticates this entity, i.e. verifies that an entity really is the one it claims to be.

These identification and authentication procedures may be performed at various stages of the communication process, or before the access to various machines in the network.

2.5.2 Types of information threatened

A public network offers various resources to network entities. Such resources may be databases, mailboxes, etc., but also all kinds of services may be considered as such resources for our purposes here.

It is clear that not every entity, even after the identity of this entity has been verified by authentication, may use any resource at their discretion. The use of a specific resource by an entity is only possible if it is authorised to do so in a specified and precise way, i.e. if it has the correct access rights needed for the intended use of that resource.

In the case of a database, such access rights may be the right to read, to update or to delete the information. It is the task of access control to ensure that entities which want to access a resource have the proper access rights. So, not only the identity of an entity needs to be verified, but also its access rights.

2.5.3 Point of attack and originator of the threat

When masquerading an entity, a fraudster tries to impersonate another entity to get the same rights and facilities as the masqueraded entity.

The point of attack can be anywhere on the link between the entity to be masqueraded and the entity to be connected. It can also come from the location of another network entity sending information simulating another entity.

2.5.4 Risks due to masquerading as another entity

When masquerading as another entity involved in CCS#7 management, an entity can:

- get unauthorised access to sensitive signalling information ,
- get unauthorised use or access rights to equipment.

By getting unauthorised access to sensitive signalling information, either accidental access or intentional access, the non-authorised entity can then endanger the confidentiality and the integrity of the accessed information.

The risks due to this threat are thus the risks due to loss of integrity or corruption of signalling data and the disclosure and loss of confidentiality of signalling data. These risks are described in the above and following subsections.

In the prevention of accidental and intentional masquerading or unauthorised access related threats, authentication services should be implemented in order to verify that the peer CCS#7-entity is the one claimed. Then, only after a successful authentication of the parties involved in the signalling exchange, confidentiality and integrity services should be provided in the establishment and maintenance of a secure signalling channel. Moreover, some authentication techniques can be used to provide the security parameters and required keys used in the management of this secure CCS#7 channel.

Moreover, access control techniques are closely related to masquerading prevention techniques and unauthorised access related threats. Access control techniques should also be invoked immediately after a successful authentication.

2.6 Threats related to eavesdropping or disclosure of information

2.6.1 Description

Confidentiality of data means that the data have not been disclosed, in the process of communication or while being stored, without the permission of its owner.

However, in many cases in the protection of the CCS#7, intentional eavesdropping of information may not be detected in real time. Only protection against ease of eavesdropping can be provided, in such a way that the recovery of original information by an eavesdropper needs large amount of money, computer capabilities and time.

2.6.2 Types of information threatened

The threats related to the loss of confidentiality are quite different according to the type of data (transmitted data or stored data) threatened. The countermeasures to protect against loss of confidentiality may also be different. For example, the protection of stored data against disclosure may be covered by a combination of access control and authentication services, whereas the protection of transmitted data against disclosure may be done by implementation of encipherment mechanisms.

Transmitted data: it is not sufficient to only protect individual CCS#7 messages against accidental disclosure or intentional eavesdropping. The complete set of signalling operations that must necessarily be performed in order to communicate successfully between two entities need to be covered and protected.

Stored data: the information contained in a database may be used by other parties in such a way as to damage the interest of the administration owning the information.

Both accidental and intentional disclosure of the transmitted or stored information can be prevented by adequate cryptographic measures with a very high probability. But, the detection of any loss of confidentiality of CCS#7 data is very difficult in real time.

The internal structure of the area of the database to be accessed by other networks databases may need to be disclosed but this is dependent on the type of function performed, e.g. copying. Disclosure of the structure of a database may not be considered as a threat. However, loss of confidentiality for the contents of the CCS#7 data (disclosure to unauthorised entity) should be avoided.

Moreover, differences in security policy of networks may result in accidental disclosure of information. For example the security policy of one CCS#7 network may be undermined by the security policy of another CCS#7 network when data is transferred (e.g. service profile information).

National regulatory requirements concerning the protection of data also need to be considered.

2.6.3 Point of attack and originator of the attack

The intrusion of an attacker in the fixed network may be difficult to realise, but it is by no means impossible for a dedicated intruder.

The identification of the most sensitive access points is one of the key points before any efficient security policy implementation.

In the case of intentional threat, an attacker tries to eavesdrop transmitted CCS#7 information or to read stored CCS#7 data.

The attacker may try either to impersonate another entity in order to get the same access rights to sensitive CCS#7 data as the masqueraded entity, or to intercept information when transmitted on a specific link.

The point of attack can be somewhere on the link where information is transmitted, i.e. between the entities exchanging sensitive data. It can also come from the location of another network entity sending or receiving sensitive CCS#7 information.

2.6.4 Risks due to disclosure of information

The loss of confidentiality of signalling data is not considered to be as risky as threats related to loss of integrity or unauthorised access to the CCS#7 network. However, threats related to loss of confidentiality may sometimes be considered as risky threats for the CCS#7. They result in some critical scenarios for a network operator.

Similarly, loss of confidentiality of information which would then enable services to be used fraudulently is considered to be very risky for the operator. Indeed, the loss of confidentiality of charging information may provide a free use of services for a specific user or subscriber (e.g. for the attacker/eavesdropper).

Accidental threats: in the case of accidental loss of confidentiality of data by an entity, the profit for the receiving entity is not straightforward. If the disclosed data is of no use to the receiver or can only be used by the original owner, the profit for the receiving entity is usually nil.

Of course, this profit may be high if the disclosed data is delivered in a profitable form, but as it has not been done intentionally, the receiving entity must also, in order to get some profit from the data he has recovered, accidentally take advantage of it. or take the opportunity of this accidental disclosure to fraudulently take advantage of it. Hence, in case of an accidental disclosure of information, the profit for the receiving entity may be very low.

But, the damage caused indirectly by this accidental modification of data, may be very crucial and severe. Actually, accidental disclosure of data may result in the broadcasting of information stored in databases like user profiles, subscriber identities, and charging information related data.

This may also result in the replaying of sensitive understandable signalling messages to other messages disturbing the functionalities and the capacities of the whole network, creating congestion of links and equipment... But in this case, not only eavesdropping CCS#7 information in the network is needed, but also broadcasting messages in the CCS#7.

Intentional threats: in case of the intentional attack, the profit for the attacker is generally the ability to get free access to a service or network, or more rarely to jam a network, to cause denial of services to specific users, or to sabotage the whole network. The damage to the operator is then mainly a loss of revenue.

However, eavesdropping and recovery of sensitive CCS#7 information may be very useful for an attacker trying to sabotage the functionalities of a network or trying to engender within the subscribers a loss of confidence in the reliability and availability of the network.

The potential consequences of accidental or intentional loss of confidentiality of sensitive information may be the reason for the implementation of adequate countermeasures in the CCS#7.

The confidentiality services to be implemented as adequate countermeasures against threats related to disclosure of transmitted data are only useful if the communicating parties are authenticated. The authentication can be used for providing security parameters and the required keys in order to obtain a secure CCS#7 channel.

2.7 Identification of the most sensitive access points

In the protection of the whole telecommunication network, and more particularly in the maintenance of the availability of the whole telecommunication network, the availability of all signalling systems and more particularly the availability of the CCS#7 is of major importance.

Of all the telecommunication channels linking telecommunication equipment belonging, or not belonging, to the same network operator, the signalling channels are the most sensitive ones.

As a matter of fact, the consequences of attacks on the traffic channels has no concrete influence on the availability of the whole network. Elements of the signalling links, and especially the CCS#7 elements, then remain the main access points for an attacker to sabotage the network or remain the main originating points for an entity to accidentally cause trouble in the network.

In the identification of threats to the security of CCS#7, both the interface between nodes belonging to different signalling networks and the interface between nodes of the same signalling network must be investigated. These sensitive interfaces are the following ones:

- *signalling interface between two nodes or equipment belonging to the same network.* Access to such interface is quite difficult for an attacker who does not belong to the network operator. Moreover, it requires a high level of technical knowledge and the use of adequate material. However, all these difficulties can be overcome by an employee of the network operator.
- *signalling interface between nodes or equipment belonging to different networks.* This also includes the interface between two different networks. This point is of

high importance because, although the number of external interface is at present quite limited, this number should increase in the near future. Access to this interface is the result of an attack performed from the network of another operator or from an open access to the equipment of a service provider.

From the above, it can be seen that to ensure that the integrity and the availability of network data is not compromised via direct access across a network boundary, security mechanisms are required. This applies to the signalling link which carries the information as well as the storage of, and access to, sensitive information.

3 Protocol analysis

The signalling system no. 7 consists of a protocol stack which is made up of some different protocols: MTP, SCCP, TCAP, ISUP and other User Parts. For the purposes of this study the protocols MTP and SCCP are considered because the other protocols do not contain or treat information that could significantly jeopardise the signalling network, but information which involves the telecommunication service. The analysis of such protocols leads to the identification of messages and parameters carrying information of particular importance, that should be considered for the control of the access to the own signalling network.

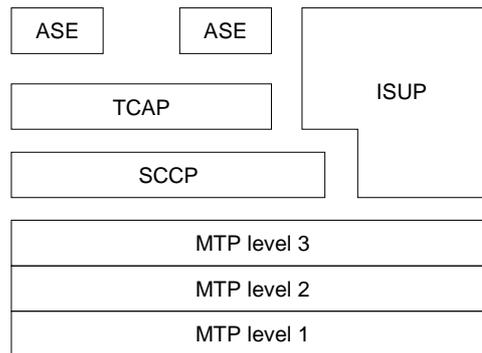


Figure 3.1 - The Signalling System no. 7

In this chapter, taking into account the threats identified in the previous section, for the two protocols MTP and SCCP will be listed:

- The main messages and parameters (together with information elements and fields) that may produce consequences in the signalling system in the case of inclusion or alteration. Elements related to the control of only one call may be considered as less important, while elements related to the control or management of the whole network must be considered as very dangerous. The embedding of these two kinds of elements in the signalling system no. 7, and the consequences on the security of the whole network should be investigated very carefully.
- The corresponding access points (intra-network or inter-network access points) at which it is possible to receive such messages. In fact in our analysis we considered only incoming messages.

3.1 MTP

The analysis focuses on MTP-3 level. The lower levels (MTP-2 and MTP-1) do not “understand” most of the information carried by MSUs (Message Signal Unit) and are only involved in the reliable transfer of the messages between the two extremes of the link.

The main task of MTP-3 is the routing of messages through the signalling network; for this reason it contains information related to the network topology (i.e. routing tables). Such information can dynamically change by means of the *network management* functions inside MTP-3.

For this purpose, at the interface with another operator or service provider, particular attention must be given to level 3 network management messages because they can access and modify the routing information of the network. Moreover, “normal” MSU, carrying information from the User Parts, must be checked to avoid illegal access and use of the network.

With regard to the access points interfacing with another network, the nodes which offer transfer capability (STP) and which act like relay points (SCCP relay point) should be considered with particular care.

3.1.1 User part messages

These messages are exchanged between user parts (i.e. by SCCP and ISUP) using the transport capacity of MTP. This is the higher signalling traffic share and the diversion of traffic towards another network could result in some problems in the network overloaded by the unexpected traffic; furthermore MSUs could not be authorised to go through one’s network.

For these reasons, and to have good control of the access to the ‘own’ network, incoming MSUs should be checked.

3.1.2 Management messages

These messages are generated by the MTP-3 level in order to maintain the signalling service and to restore normal signalling conditions in the case of failure, either in signalling links or signalling points. To accomplish this task MTP has three signalling network management functions:

- *traffic management*: it is used to divert signalling traffic from a link or route to one or more different links or routes, to restart a signalling point, and to control congestion;
- *link management*: it is used to restore failed signalling links and to activate and deactivate signalling links;
- *route management*: it is used to distribute information about the signalling network status.

These functions use particular messages, management messages, to inform the nodes of the network on the abnormal situation, and to re-route, if possible, the signalling traffic. It is obvious that such messages, that can re-route the traffic, constitute one of the means of threats to endanger the integrity of the signalling network.

Looking at network integrity, messages carrying relevant security information can be split into two categories:

- messages communicating unavailability (e.g. CO, ECO, TFP, TFR, MIM, TFC);
- messages communicating availability (e.g. CB, TFA).

It is obvious that the first category has a higher degree of risk, and more care should be given to the treatment of such messages.

In the following, a list is given of the management messages that carry information relevant to network integrity. A description of risk related to their handling is listed as well.

3.1.2.1 Changeover (CO) and Emergency Changeover messages (ECO)

These messages are used to divert the signalling traffic directed to a destination from an unavailable link to an alternative one. When such messages are exchanged between two nodes MSUs use new routes which use new links and/or signalling points. Therefore, the public operator must be sure that these orders come from a node or a network allowed to perform such an operation, and not from someone else who is trying to “attack” the network. Moreover, COO messages could be used when MTP level 2 fails, according to recommendation ITU-T Q704.

3.1.2.2 Changeback message (CB)

This message is used to declare that the unavailable link is newly available and the signalling traffic can be diverted from the alternative link to this one. With respect to the changeover message, less risks are related to the changeback message due to the recovering function performed.

3.1.2.3 Transfer-prohibited message (TFP)

This message is sent by a signalling transfer point (STP) to notify one or more adjacent signalling points (SP) that they must no longer route the messages towards a particular destination via that STP. By sending this message, a node does not permit other nodes to use its transfer capability for signalling messages destined to a particular node. The TFP produces a routing reconfiguration and traffic diversion.

3.1.2.4 Transfer allowed message (TFA)

This message is sent by a STP to notify one or more adjacent SPs that they can route traffic towards the specified destination using the STP. As for all messages which are used in recovery function, less risks are related to the exchange of such messages.

3.1.2.5 Transfer restricted message (TFR)

This message is a “national option” and has a preventive function. It is used by an STP to notify one or more adjacent SPs that they should, if possible, no longer route the traffic towards a specific destination via that STP. Usually, an STP sends TFR messages when, due to a long-term failure such as equipment failure, it has to route traffic using particular routes normally not used. Risks coming from the receiving or sending of this message are those related to the routing reconfiguration and traffic diversion.

3.1.2.6 Management inhibit message (MIM)

MTP-3 uses this message when management functions request, for maintenance or testing purposes, to make or keep a signalling link unavailable to user part signalling messages. This message does not cause any link status change at level 2, so the link will be able to transmit maintenance and test messages. As the management inhibiting acknowledge message results in a time controlled changeover, risks related to reception or sending of such messages are the same as CO and CB messages.

3.1.2.7 Transfer controlled message (TFC)

This message is used during a congestion situation to convey the congestion indication. The TFC message is sent by the STP where congestion is detected to the originating SP. Different options, that lead to different behaviours in the receiving end, are available: international, national with congestion priorities, national without congestion priorities. The TFC messages do not cause the use of new routes, but only a reduction in the traffic load.

3.1.3 Parameters

Not the whole MSU carries information which can threat the integrity of the signalling network or can be used to verify the correctness of information received. For the mentioned messages, only part of them should be checked. In general, information of interest is the addresses of origin and destination, to verify that the originating end is entitled to exchange messages with the destination end. For this reason the following parameters should be taken into account (see figure 3.2):

1. *Originating point code (OPC)*: this parameter is the physical address of the originating node and is included in the routing label. A verification of the correctness of the OPC (for example by verifying an authentication code accompanying that OPC), and of the rights of the corresponding node, should be done to verify that the node sending the message can route via the node which is in charge of the check. This can be done, for example, by checking that the node is present in routing tables and/or by using cryptographic mechanisms proving that this node is the one claimed.
2. *Destination point code (DPC)*: this parameter is the physical address of the destination node and is included in the routing label. A check on the DPC should be done to verify that:
 - normal MSUs, coming from an external node, are addressed to a node inside one's network (to avoid the use of the network as a transit network for MSUs);
 - management messages, coming from an external node, are addressed to a node at the interface between the networks (management messages should only involve interconnecting nodes at the interface with other networks and not other parts of the signalling network itself);

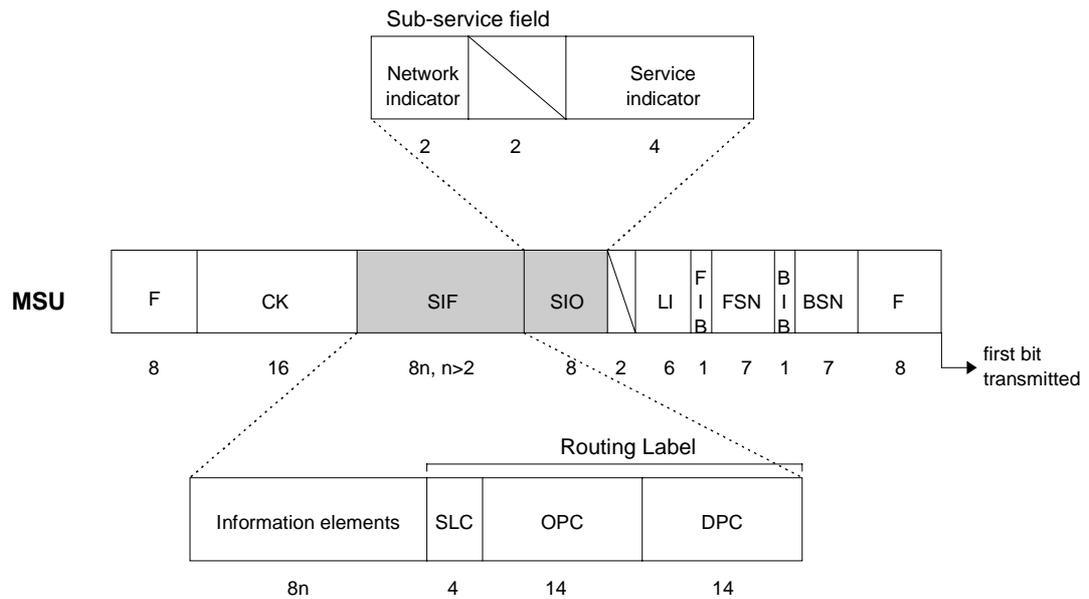


Figure 3.2 - MSU structure

3. *Service indicator (SI)*: this parameter, inserted in the *service information octet (SIO)*, is used by signalling handling functions to perform message distribution and in some special applications to perform message routing. It identifies the relevant user part.
4. *Network indicator (NI)*: this parameter, inserted in the *service information octet (SIO)*, is used by signalling handling functions to distinguish between international or national MSUs. Control mechanisms should be applied only to international MSUs.
5. *Information field (SIF)*: this field contain the signalling information inserted by the relevant user part or by MTP-3 itself for management messages. For the integrity of the signalling network only the information field of management messages should be checked because in that case it contains information that influences the routing of messages.

Table 3.1 summarises the reasons that lead to the control of messages and parameters at MTP level.

Messages	Parameters	Reasons
Normal MSU (in case of an STP)	OPC	verify that the originating node is known (i.e. it is present in the routing tables). This is normally NOT done in an STP node, but could be useful to prevent unauthorized access to the network
	DPC	verify that the message is destined to a valid node (i.e. a node to which the originating point is allowed to route)
Changeover, Changeback and Emergency changeover	OPC	verify that the message is received from a node allowed to send this type of messages. The allowed node list should be chosen by the operator according to particular needs/threats
	DPC	verify that the message is destined to itself or to another node interconnecting the two networks
Transfer Prohibited, Transfer Restricted	OPC	verify that the message is received from an adjacent node allowed to send that type of messages
	information field	the destination to which the message refers must be a node in the same network of the originating point
Management Inhibiting	OPC	verify that the message is received from an adjacent node allowed to send this type of messages
Transfer Controlled	OPC	verify that the message is received from a node allowed to send this type of messages. The allowed node list should be chosen by the operator according to particular needs/threats
	DPC	verify that the message is destined to a node to which the originating node can route traffic
	information field	the destination must be a signalling point of the same network of the originating point

Table 3.1 - MTP messages and parameters

Moreover, all messages, both normal MSU and management messages, should be verified that the message is received on a “valid” linkset: the originating point is allowed to use that particular linkset.

3.2 SCCP

As for MTP, messages arriving both from upper layers and management messages generated by SCCP are of interest. Particular attention has to be given to those nodes which have SCCP Relay Point functionality, because, after the translation of Global Title, the following nodes would not be able to identify the real origin of messages.

In particular, UDT (Unit Data) and XUDT (eXtended Unit Data) messages should be checked. Their format is depicted in fig. 3.3. These messages are used to carry information coming from upper levels and for management purposes; the difference is in the content of the data field that is either the TCAP information or the identity of a subsystem experiencing a failure.

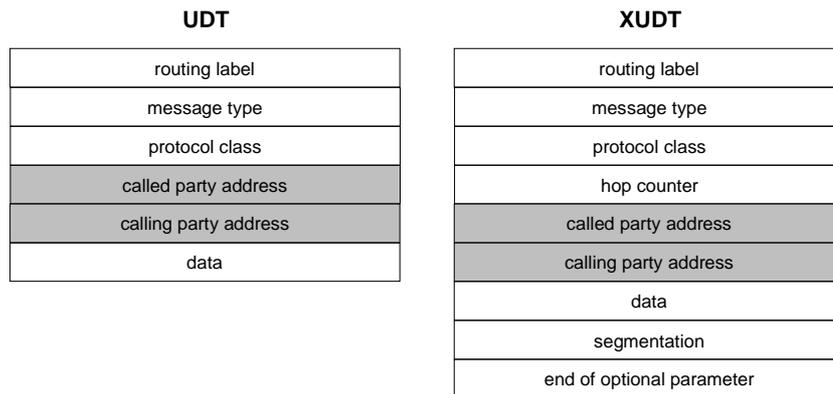


Figure 3.3 - UDT and XUDT message format

3.2.1 Upper level messages

These messages come from TCAP level and are related to offered services (e.g. intelligent services, mobility services); such messages make much use of the GTT functionality.

The translation of the Global Title is a “huge” operation and an abnormal use of it could damage the performance of the node. For this reason there is the need to check both the applicant and the result of the translation so as to avoid illegal use of SCCP Relay Point functionalities.

3.2.2 Management messages

These messages are generated by the SCCP level in order to maintain network performances by re-routing or throttling of traffic in the event of failure or congestion in the network. To accomplish this task SCCP is organised into two subfunctions: signalling point status management and subsystem status management.

These procedures rely on indications provided by MTP (MTP-PAUSE, MTP-RESUME AND MTP-STATUS) and on information received in SCCP management messages. Such messages allow the two management functions to inform the nodes of the network of the abnormal situation, and to re-route, if possible, the signalling traffic. It is obvious that these messages, that can re-route the traffic, constitute the means by which the integrity of the signalling network at SCCP level can be penetrated and endangered.

In the following are listed management messages that carry information relevant to network integrity; the related risks are described as well. In Figure 3.4 the format of the data field of UDT messages used for SCCP management is depicted.

	nr. of octets
SCCP management message format id.	1
affected SSN	1
affected PC	2
subsystem multiplicity	1

Figure 3.4 - Data field format of SCCP management messages

3.2.2.1 Subsystem prohibited (SSP)

This message is sent by a local SCCP to inform a remote SCCP management of the failure of a subsystem. The receiving end of an SSP message will update its translation tables; as a consequence traffic could be re-routed to a backup subsystem. Connected to the receipt of this message there is the risk of an SCCP user being no longer able to offer a particular service. Therefore, the operator must be sure that this message comes from an allowed node (and network), and not from someone else who is trying to attack the network.

3.2.2.2 Subsystem allowed (SSA)

This message is sent by a local SCCP to inform a remote SCCP management that a subsystem previously prohibited is now allowed. The receiving end of an SSA message will update its translation tables; as a consequence traffic is newly routed to that subsystem. Less risks are related to the receiving of this message because it carries information of availability.

3.2.2.3 Subsystem status test (SST)

This message is sent by a local SCCP to verify the status of a remote subsystem marked prohibited or the status of a remote SCCP marked unavailable. The receiving end of an SST message checks the status of the named subsystem and, if the subsystem is allowed, an SSA message is sent in response. If the subsystem is prohibited, no reply is sent. Particular care has to be taken to verify the originating node (that must have the rights needed).

3.2.3 Parameters

Not the whole message has to be checked in order to allow access to one's network. Those parameters which identify the origin and the destination of the message and those that take part in the translation of the GT have particular importance.

In the following, the relevant parameters and field are listed:

1. The *calling party address*: this parameter contains enough information to uniquely identify the origination signalling point. This address may contain the signalling point code, the Global Title and the subsystem number; the mix of such items is made according to the coding of the *address indicator* octet (see Figure 3.5).

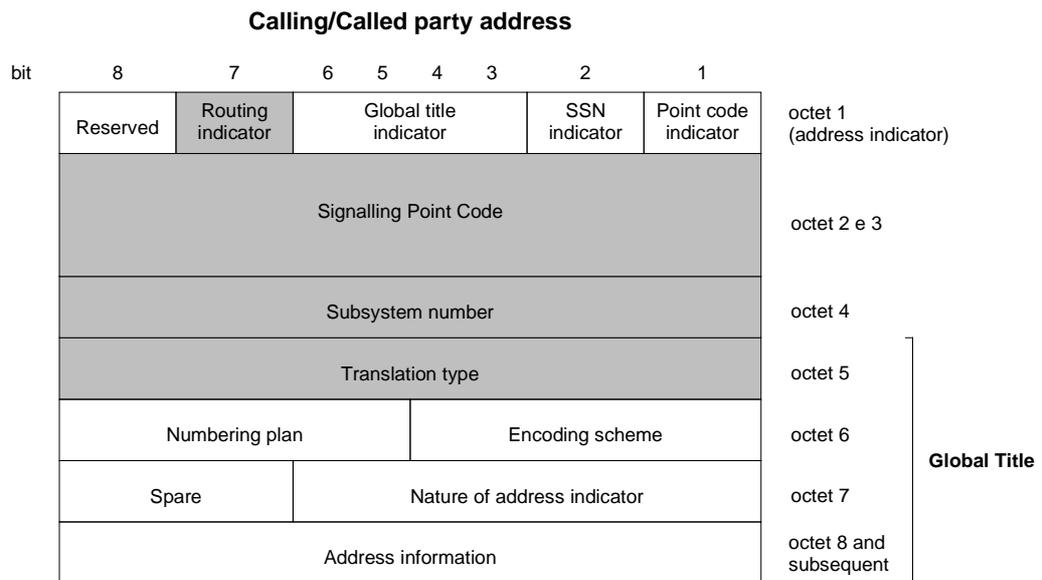


Figure 3.5 - GT information present in the calling/called party address

- The *Called Party Address*: this parameter contains enough information to uniquely identify the destination signalling point. This address has the same format as the calling one (see Figure 3.5).

Two routing alternatives, based on the value of the address indicator, are possible:

- routing based on the Subsystem Number: the message does not need a translation (i.e. the node is the destination of the message) and the SSN (Subsystem Number) is screened against the values in the Calling Party Address;
 - routing based on Global Title: the message needs a translation and the “Translation Type” should be screened against the value in the Calling Party Address field, to verify that a particular origin has the necessary rights to access the translation tables. After the translation has been done, an additional check on the results is required: the new DPC and the new SSN should be verified against the values in the Calling Party Address field.
- The *Affected Point Code* (see figure 3.4): this parameter identifies a signalling point where the affected subsystem is located. This field, which has to be checked together with the Affected Subsystem Number, must indicate a Point Code (PC) to which the node can address SCCP messages.
 - The *Affected Subsystem Number* (see figure 3.4): this parameter identifies the SCCP or a subsystem which is failed, withdrawn, congested, allowed or tested (depending on the type of the message: SSP, SSA or SST). It must indicate an SSN, together with the affected PC, to which the node can address SCCP messages.

Table 3.2 summarises the reasons that lead to the control of messages and parameters at SCCP level.

Message	Parameter	Reasons
UDT and XUDT	Calling Party Address	verify that the message is received from a specified remote subsystem (i.e. a specified combination of SSN+SPC or GT)
	Called Party Address	for routing on SSN: verify that the message is destined to a local subsystem
		for routing on GT: verify that the message uses a valid translation table (i.e. a table allowed for the origin)
	Results of the translation	verify that the new values of DPC and SSN are matching with specified values for the origin of the message
SSP and SSA	Calling Party Address	verify that the message is received from a specified remote subsystem (i.e. a specified combination of SSN+SPC or GT)
	Called Party Address	verify that the message is destined to the management of SCCP (SSN=1)
	Affected point code	verify that the affected node is inside the originating network
	Affected subsystem number	verify that the affected subsystem is known
SST	Calling Party Address	verify that the message is received from a valid remote subsystem (i.e. a valid SSN+SPC or GT)
	Called Party Address	verify that the message is destined to the management of SCCP (SSN=1)

Table 3.2 - SCCP messages and parameters

4 Integrity mechanisms for the CCS#7 system

Sometimes, it is not sufficient to check that the received information, like OPC of the CCS#7 entity, is known (i.e. belonging to appropriate tables). It is sometimes necessary to verify the correctness of this information; that is to say, to verify that the code received is the right one and has not been changed or masqueraded. The use of security mechanisms is thus needed.

4.1 Overview of integrity services

Integrity is defined as the property that data has not been altered or destroyed in an unauthorised manner. The integrity services considered for the protection of the CCS#7, are services by means of which the information transferred or stored has not been altered or destroyed in an unauthorised manner at the transmission lines or databases (see also [8]).

Two classes of integrity services for the CCS#7 can be distinguished. Namely:

1. *Class one: detection* of unauthorised manipulation of CCS#7 related data (without recovery). These integrity services mainly notify the CCS#7 entities, to which the service is provided, of an integrity failure. This notification may result in an explicit notification of the receiver and/or the sender and eventually in the dropping of the compromised block of data or message. However, a recovery mechanism may be provided by higher layer functions in addition.
2. *Class two: protection* against unauthorised manipulation of CCS#7 related data (with recovery). Class two may also imply that it should be possible to hold the communication flow and perform a recovery procedure.

An integrity service is usually implemented in such a way that an appropriate protocol sublayer at the sending entity side performs the following actions:

- subdivision of data to be transmitted in appropriate blocks,
- adding redundant information to these blocks,
- provision of cryptographic protection against accidental or intentional alteration.

At the receiving entity side, there has to be a corresponding protocol sublayer which has to check the integrity of the received data, report the result to the protocol layer above and remove the redundant information.

For certain types of message, the timing relationship between consecutive messages is important. Due to the necessary time needed to perform integrity protection at one side and verification at the other side, the implementation of integrity services in CCS#7 may then create problems. Integrity service may then not be needed for all types of communication.

The integrity protocol has to be embedded into CCS#7 protocols: Appropriate protocol layers at which the integrity protocol will be located have to be identified as well as corresponding protocol end-points where the integrity protocol can be terminated. Furthermore, an appropriate subdivision into blocks has to be defined.

The integrity services must allow the detection of modifications of the message, including the insertion, deletion, transposition or modification of the information

stored and/or transferred, detect modifications of the sequence of messages and to permit the verification of the origin and destination of the messages.

The integrity services relate to authentication service as the integrity service is only useful if the CCS#7 entities in communication are authenticated. The authentication may also be used for providing security parameters and the required keys in order to obtain a secure channel.

4.2 Integrity mechanisms

Security mechanisms may be considered as building blocks for the definition of protocols. Security mechanisms are logic or algorithm that implements a particular security enforcing or security relevant function in hardware or software (see also [12]).

According to [8]: ISO/IEC JTC1/SC 21 N 6690 (Working Draft Integrity Framework), the integrity mechanisms can be classified as follows:

- *Integrity provision through access control*: is the prevention of unauthorised use of a resource, including the prevention of use of a resource in a unauthorised manner. [9];
- *Integrity provision through encipherment* (of messages with redundancy): is the cryptographic transformation of data to produce ciphertext [9];
- *Integrity provision through MAC* (Message Authentication Code): a message authentication code (MAC) is a data field used to verify the authenticity of a message [10]. It is a key dependent one way hash function. Only someone possessing the identical key can verify the hash of this function;
- *Integrity provision through digital signature*: a digital signature is a data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient [9].

The integrity mechanisms used for the protection of stored data may be access control based mechanisms, MAC based mechanisms or digital signatures. The integrity of transmitted data may be achieved via MACs techniques, digital signatures or encryption of messages with redundancy.

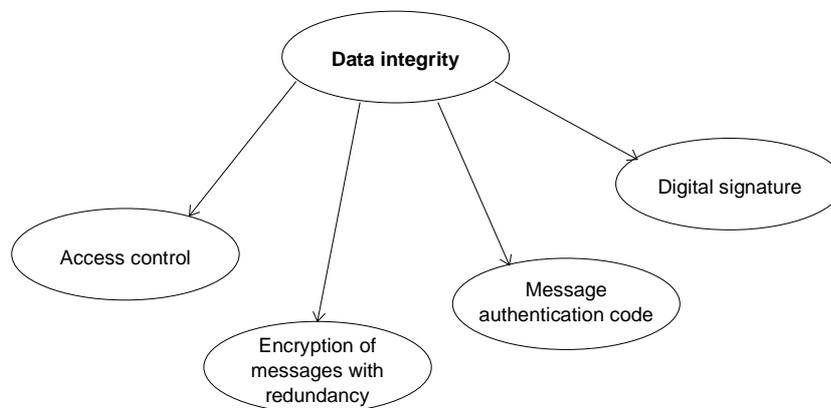


Figure 4.1 - Different classes of integrity mechanisms

The integrity mechanisms we introduce in this section are already defined in a generic way in ISO and ITU. We investigate which of these security integrity mechanisms may be well suited for CCS#7 purposes.

In order to clearly describe the type of integrity provision used in the protection of CCS#7 data, we try to provide the following information for each type of integrity mechanisms; namely:

- What is the role of this integrity mechanism?.
- What is its cost?.
- What is the performance of this mechanism?.
- What are the risks that are not covered by this mechanism?
- What is the required infrastructure to provide such a mechanism?.
- What are the precautionary measures to be taken in case of multiple use?.
- What are the lawful requirements regarding to this mechanism?.

4.2.1 Integrity provision through encipherment (for transmitted data)

4.2.1.1 Introduction

In the special case of a very high redundancy of the transferred data, encipherment may provide enough assurance that the transmitted data has not been modified. Due to the high redundancy of speech data, confidentiality based techniques often provide enough assurance of integrity for voice/speech. However, the general usefulness of such techniques for providing detection of integrity failure for all CCS#7 messages is not clear. However, for some specific CCS#7 data, these techniques which can provide good performance for detection of integrity failure, may be needed.

Encipherment-based integrity mechanisms are based on symmetric (i.e. secret key) encipherment techniques. The same secret key is used to protect the data, i.e. to cipher them, and to verify their integrity. Then, the most important aspect of these secret key techniques is that the set of entities (CCS#7 entities, machines, operators...) capable of receiving integrity-protected data must be limited in size to the set capable of sending it.

These techniques enable the detection of the modifications made by a third entity (person, machine,...) on data transferred between two entities. These encipherment-based integrity techniques do not prevent attacks based on replay where data previously authenticated are sent again or are replacing other data enciphered by the same secret key. Some additional precautionary measures, such as the use of time stamps, random numbers or counters must be taken.

4.2.1.2 Characteristics of encipherment-based integrity mechanism

In the following, the characteristics of the encipherment mechanism are described:

-) *Role*: detection of fraudulent modification of transferred or stored data (only if data has a lot of redundancy).
-) *Cost*: not more than the cost for provision of confidentiality mechanisms.

-) *Performance*: integrity mechanisms are provided by encipherment. If the encryption mechanisms are already implemented, no supplementary time is needed to implement these mechanisms. If the basic confidentiality mechanisms are not provided, the performance is the performance of the corresponding encryption mechanisms.
-) *Risks*: these mechanisms do not prevent attacks based on replay, where data are sent again or are replacing other data enciphered by the secret key (i.e. messages may be subject to replay during the period of validity of the secret key used for encipherment). Some additional precautions, such as the use of time stamps, random numbers or counters ..., must be taken.
-) *Infrastructure*: the same infrastructure as the one needed for implementation of the corresponding encipherment mechanisms is required.
-) *Multiple use*: precautions such as time stamps, random numbers or counters must be used in order to avoid attacks based on replay.
-) *Interdependencies*: these integrity mechanisms are highly dependant on the corresponding encipherment mechanisms on which they are based.
-) *Law*: laws related to integrity mechanisms through encipherment are highly dependent on the laws related to encipherment.

4.2.2 Integrity provision through MACs and MDCs (for transmitted data)

Because of their low complexity of implementation, their good performance and the level of integrity assurance that they can provide, these techniques seem to be the most appropriate ones for the provision of integrity services in CCS#7.

4.2.2.1 Introduction

We distinguish two basic kinds of cryptographic techniques for achieving message integrity. Namely:

- *MAC*: in this case, a quantity is generated, the Message Authentication Code (MAC), which is a cryptographic function of the data and of a secret key.
- *MDC*: in this second case, another quantity, the Manipulation Detection Code (MDC) is generated, which is only a public one way hash function of the data of the message.

4.2.2.2 Principle of integrity provision through MACs

The involved mechanisms are based on a public algorithm $A(k,M)$, where k is a secret key which is shared by the sender and the receiver of the message M . The message M to be authenticated can be of any length. The function (i.e. the algorithm) A must depend on all the bits of the message. The value of such a function is called the MAC of M . This MAC is appended to the message M when it is sent. The receiver checks the validity of the MAC by means of the secret key k . He calculates $A(k,M)$ and compares it with the received value. If the values are equal, the message is accepted and it is supposed to be originating from the claimed entity¹.

¹ A MAC can also be used to secure stored data. The entity who knows the secret key is then able to check that the stored data has not been modified.

As well as for integrity services through encipherment, the utilisation of a MAC does not enable the detection of attacks based on replay, where data previously authenticated are sent again or are replacing other data with their associated MAC. Some additional precautions, such as the use of time stamps or counters must be taken.

There are several problems with the use of the MAC techniques, for instance in the case of block messages. It is useful in signalling messages but the requirement of a special space for the message digest might be a problem for the optimisation of the efficiency.

4.2.2.3 Remarks concerning the use of MDC

The MDC only takes into account the data to be protected, and does not consider any secret key.

The function used in the elaboration of an MDC is a public one way hash function. There is no key to prevent a third party making an MDC for a known message. So, it is necessary to encrypt the overall message or only the MDC of the sent message, in order to be sure that the sent message has not been substituted during transmission.

If the overall message is encrypted, secrecy as well as integrity is achieved. If only the MDC is encrypted, this is logically equivalent to an MAC calculation.

4.2.2.4 Characteristics of MACs and MDCs - based integrity mechanisms

In the following, the characteristics for MAC and MDCs mechanisms are described:

- a) *Role*: detection of fraudulent modifications of transferred or stored data.
- b) *Cost*: the cost of these mechanisms depends on:
 - the cost of the function A;
 - the increase of the amount of data to be transferred (depending on the size of the MAC to be appended to the message).
- c) *Performance*: the time needed depends on the time needed for computation of the value $A(k,M)$ or the MDC and the following encryption process.
- d) *Risks*: these mechanisms do not prevent attacks based on replay, where data previously authenticated are sent again or are replacing other data (i.e. messages may be subject to replay during the period of validity of the secret key used for MAC). Some additional precautions, such as the use of time stamps, random numbers or counters must be taken.
- e) *Infrastructure*: the infrastructure must enable the management (creation, distribution, ...) of the secret key used for the elaboration (resp. verification) of the MAC by the sender (resp. receiver) of the message, or the cipher key used to encrypt the MDC or the message including the MDC.
- f) *Multiple use*: precautions such as time stamps, random numbers or counters must be used in order to avoid attacks based on replay.
- g) *Interdependencies*: the usefulness of the implementation of such mechanisms depends on the efficiency of authentication mechanisms provided to authenticate the sender and receiver of the message to be protected.

- h) *Law*: laws related to integrity are highly dependent on the laws related to encipherment.

4.2.3 Integrity provision through digital signature

4.2.3.1 Advantages of digital signature schemes

Digital signatures can also provide integrity service. Digital signature schemes allow information to be transformed using a secret parameter in a way that only its possessor could have done, but with the information being recoverable by anyone by means of a corresponding public parameter.

These mechanisms could be used along with other minor techniques for providing authentication and the rest of security services required to the network. The X.509 standard of CCITT provides a good framework for these purposes.

It is out of the scope of this Project to describe these techniques in detail. For more information on this subject, a complementary description of public key techniques can be found in the X.509 standard.

Besides the digital signatures, in the chapters above we defined integrity mechanisms based on symmetric keys (both originator and receiver of the message know the secret key and they are both able to generate the message authentication code). The secrecy of the common (shared) key protects them against active attacks performed by a third entity, but this does not protect one entity from the other entity. Disputes may arise between originator and receiver of a message.

For example the entity A can send a message (accompanied by its corresponding Message Authentication Code) to the entity B. But, if B is a dishonest entity, it is then able to produce a different message, claiming that this new message originates from A.

So, the MAC cannot be used to solve this kind of dispute, as A can deny having sent a message that has been received by B and as B can modify a message and claim that A sent it.

Digital signatures can be used to solve such disputes.

4.2.3.2 Performance aspects of integrity mechanisms using digital signature schemes

Digital signature schemes may be used to provide data integrity. This is done by providing a signature on a hash value of the message to be protected. In general, the comparatively low performance of implementations of digital signature schemes does not translate into a low performance of integrity mechanisms using digital signature schemes as the length of the hash value is fixed for arbitrary message lengths.

However, the probability that the integrity of a message is violated due to random bit errors increases with the length of the message. This may lead to a maximum admissible length for a message whose integrity is protected by a single signature, and consequently to a maximum throughput for the integrity mechanism.

Digital signature based mechanisms are not appropriated for general integrity provision in the CCS#7. The complexity of implementation, the need for dedicated hardware, the length of required keys, the slowness of calculation of the corresponding algorithms, and/or verification of the digital signature do not favour the

use of digital signature based mechanisms for the provision of integrity services in a normal operation of CCS#7 message transmission. MAC based mechanisms would be then more appropriate.

However, digital signature based mechanisms provide the highest level of assurance for authentication or integrity purposes. So the use of digital signature based mechanisms may be required for very specific authentication of peer entity, or for the maintenance of a high level of integrity of specific and sensitive CCS#7 data.

4.2.4 Integrity of stored data

In the above subsections, we defined techniques for protecting the integrity of transmitted CCS#7 messages. However, in the maintenance of the availability and integrity of the network, it is of high importance that stored CCS#7 data like identifiers, identities and data in routing tables, have not been accidentally or intentionally modified. Even if this problem of stored CCS#7 data is not directly CCS#7 interconnection relevant, it is an important aspect in the maintenance of the integrity of the CCS#7 system.

The techniques for the protection of data stored temporarily or permanently, might be different from the techniques used for the protection of transmitted data. Stored data may be protected, for instance, by means of one of the following two techniques:

- access control techniques;
- authentication codes techniques.

In the CCS#7 context, integrity services provide a guarantee that information stored permanently in databases or temporarily in nodes of the network, has not been altered, destroyed, modified, created or deleted in an unauthorised manner.

4.2.4.1 Integrity provision through access control techniques

Integrity provision through access control techniques is considered to be very appropriate in case of access to sensitive data stored in databases. Access control may be used to achieve integrity by preventing unauthorised creation, deletion or modification of stored data. Only entities having valid access rights to the data can have an access to it, and can then create, modify or delete all or part of this data. Of course, other integrity mechanisms, like authentication codes based, encipherment based, or digital signature based techniques may be additionally used in combination with access control techniques.

A general description of access control techniques that may be required for the protection of integrity and maintenance of availability for the CCS#7 is provided in the above access control mechanisms related chapter.

4.2.4.2 Integrity provision through authentication codes techniques

A file of data can be protected against unauthorised modifications by means of authentication and integrity techniques, quite similar to the techniques provided for transferred data. For each file of data to be protected, message authentication codes (MACs) are calculated by means of secret keys. They are then stored with the data they are supposed to protect. The entity possessing these data also possesses the secret keys and is then able to check the value of the MACs. The use of authentication codes techniques can then be divided into two possibilities:

1. *One MAC is calculated on the whole file:* a first possibility could be to protect the whole file of sensitive data by calculating only one MAC depending on the data of the whole file. Hence, a shifting entity also has to check the MAC calculated on the whole file (that may be very large) before using one of the data. Moreover, each minor modification of the data leads to a recalculation of the MAC on the whole file.
2. *The file is subdivided into many subfiles, one MAC being calculated for each subfile:* of course, the calculation of each MAC is much shorter. However, this protection engenders a potential threat, which is the modification of the positions of each protected subfile. For instance, a defrauder may replace one of the subfiles by another one, each of them with their corresponding MACs. A modification of the positions of the different subfiles may have major consequences if, for example, the subfiles are lists of orders to be given to machines.

5 Mechanisms to avoid unauthorised use of resources

To reduce the likelihood of failure produced by an unauthorised use of the signalling network, new functionalities acting on incoming messages should be inserted in the network. These functionalities act as filters cutting unexpected messages and implementing the checks outlined in §§ 3.1 and 3.2.

Three functions have been identified as possible solutions for the problem of access control:

- *monitoring*: consists for example of a simple control of the traffic level in signalling links between the 'own' network and the others, or a call tracing, or a filtering the events in a signalling link waiting for a particular event, and so on;
- *screening*: consists of controlling, and eventually discarding, incoming messages to verify that the reasons described in §§ 3.1 and 3.2 are not violated;
- *policing*: consists of a control on the activities started outside the network and having an impact on it.

In the following, the three functions are better explained.

5.1 Monitoring of signalling traffic

The control of the level of the signalling traffic is the simplest method of revealing an abnormal use of the CCS#7 network. Control of such a level may prevent links and nodes from a misuse, either accidental or on purpose.

To implement this control function, measures of the traffic, either in terms of messages or octets, must be set on the signalling links interconnecting other networks. The measured values should be compared with a predetermined threshold for "regular traffic"; when the value on the link exceeds the threshold an alarm should be generated and more sophisticated controls, or a simple notification to the management part of the node, could be activated.

5.2 Screening of messages

Before an incoming MSU is accepted it should pass a series of verifications which assure the conformance to the criteria indicated in §§ 3.1 and 3.2. This consists of authentication, integrity and access control procedures verifications by means of appropriate mechanisms. The choice of security mechanisms to be implemented for each security domain (authentication, integrity, confidentiality, access control) depends on the security policy that has been chosen by a network operator, or that has been negotiated and agreed between two network operators. If an MSU does not pass the test it should be discarded. This kind of operation, performed on arriving messages, is called *message screening*.

As can be seen in Figure 5.2, message screening function operates both at MTP level and SCCP level.

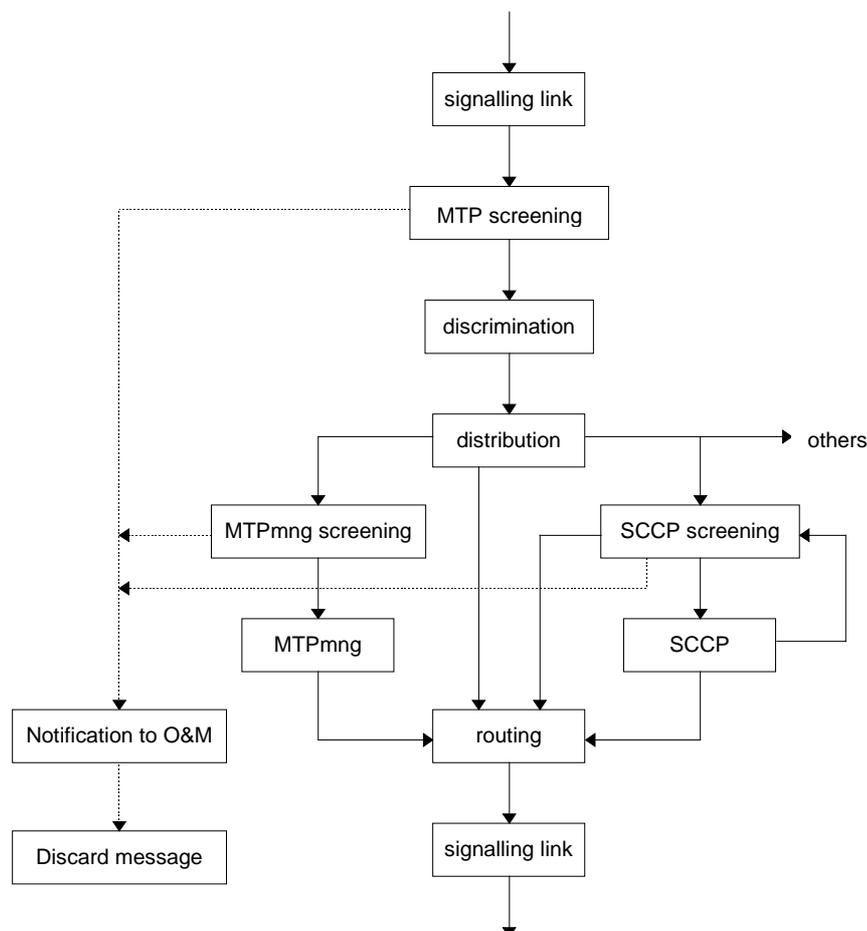


Figure 5.1 - Flow of screened messages

Messages coming from outside the network are first screened at MTP level, where the parameters are checked according to the Table 3.1. If messages do not violate the rules defined, that means verification of the correctness of parameters, these messages will be distributed to upper levels or re-routed to other destinations (STP functionality). Locally destined MTP network management messages are then screened to verify the information field (see Table 3.1). SCCP messages are screened as well, and in particular SCCP messages that need a GTT are checked either before or after the translation. This is done every time there is a violation of the rules outlined in Table 3.1 and Table 3.2.

5.3 Policing of activities

This function implies a control in the activities started by an external node and that influences one signalling network. Not all of the interconnected nodes and/or networks are allowed to perform the same operations, therefore there is the need to verify that the origin of the message has the necessary access rights (network management and test functions are typical examples of activities to be monitored). Some of the tests that could be performed are indicated in Table 3.1. and Table 3.2 summarises the reasons that lead to the control of messages and parameters at SCCP level.

5.4 Where to adopt protection mechanisms

The nodes at the interface with other PNOs can have, from the signalling point of view, four different roles: simple SP, STP, SCCP Relay Point² and STP/SCCP Relay Point.

If a node does not have STP functionality, it will be the end point for the signalling message and less severe controls are needed. In fact, when a node is the destination of the message it will only have to verify the origination and the kind of operation requested because there is no risk to involve any other nodes or networks.

Nodes with the SCCP Relay Point functionality need much more care because not only do they act as a mirror for SCCP messages, but after the translation the new destination would not be able to identify the real origin of the message (with obvious problems for the security).

In Table 5.1 there is a possible implementation of the different mechanisms formerly described in the four different types of signalling points.

	Monitoring	Screening	Policing
<i>Simple SP</i>	Always	After a first alarm from monitoring	After an alarm from monitoring
<i>STP</i>	Optional	Always	After an alarm from monitoring or screening
<i>SCCP Relay Point</i>	Optional	Always	After an alarm from monitoring or screening
<i>STP/SCCP Relay Point</i>	Optional	Always	After an alarm from monitoring or screening

Table 5.1 - Example of use of protection mechanisms

² All type of nodes can be integrated (i.e. with voice trunks) or not.

References

- [1] Recommendation X.509, ISO/IEC 9594-8, Information technology, Open Systems Interconnection, The Directory: Authentication Framework.
- [2] Recommendation X.511, ISO/IEC 9594-3, Information technology, Open Systems Interconnection, The Directory: Abstract Service Definition.
- [3] Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications.
- [4] Recommendation X811: Information Technology - Open systems Interconnection - Security Frameworks for open Systems: Authentication Framework.
- [5] ETSI STAG TCR - TR 028: Glossary of security terminology.
- [6] Recommendations 701-704: Signalling System No. 7 - Message Transfer Part (MTP).
- [7] Recommendations 711-714: Signalling System No. 7 - Signalling Connection Control Part (SCCP).
- [8] ISO/IEC JTC1/SC 21 N 6690. "Working Draft Integrity Framework".
- [9] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".
- [10] "Banking - Key management (wholesale)".
- [11] EURESCOM Project P234, Final Deliverable: "Authentication Services".
- [12] Information Technology Security Criteria Provisional Harmonised Criteria, June 1991.
- [13] Springer-Verlag/Wien, J.C. Laprie, "Dependability: basic concept and terminology" (e.d.).