TR 101 365 V1.1.1 (1998-07)

Technical Report

Intelligent Network (IN); IN interconnect threat analysis

Reference

DTR/NA-061204 (cn000ics.PDF)

Keywords

IN; security; threat analysis

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Technical Report (TR) has been produced by ETS Tecnical Committee Network Aspects (NA).

The present document is the second document in a sequence of four documents which together consider the security of the intelligent network (IN) in relation to the interconnection of two or more networks employing IN technology. The first document was ETR 339.

1 Scope

The purpose of the present document is to analyse the threats due to IN interworking between IN structured network operators and/or service providers using CS2 and CS3. A set of technical requirements will be established in a following document.

The present document analyses the attacks which could occur in the interworking relationships, the present document principally considers CS2 and will focus mainly on security problems linked to the use of SCF-SDF, SCF-SCF and SDF-SDF interfaces. These IN interfaces could be either the target of the attack or the means to perform the attack.

The present document follows the successive steps:

- listing vulnerabilities for IN architecture to the use of SCF-SDF, SCF-SCF and SDF-SDF interfaces;
- description of threats (Intentional or accidental) and their impact;
- determination of the likelihood of the attack based on the motivation of the attacker;
- production of a risk assessment.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETR 339: "Intelligent Network; IN interconnect business requirements".

[2] ITU-T Recommendation Q.1221: "Introduction to Intelligent network Capability Set 2".

[3] ITU-T Recommendation Q.1224: "Intelligent Network Distributed Functional Plane for Capability Set 2".

[4] ITU-T Recommendation Q.1228: "Intelligent Network Interface Capability Set 2".

[5] ETR 332: "Security techniques Advisory Group (STAG); Security requirements capture".

[6] ETR 232: "Security techniques Advisory Group (STAG); Glossary of security terminology".

[7] ETR 083: "Universal Personal Telecommunication (UPT); General UPT security architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

masquerade (« spoofing »): The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

unauthorized access: An entity attempts to access data in violation to the security policy in force.

eavesdropping: A breach of confidentiality by monitoring communication.

loss or corruption of information: The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.

replay of information: The repetition of previously valid commands and responses with the intention of corrupting service or causing an overload.

repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

forgery: An entity fabricates information and claims that such information was received from another entity or sent to another entity.

denial of service: The prevention of authorised access to resources or the delaying of time critical operations.

unauthorized activity: An attacker performs activities for which he has no permission or which are in contradiction of an interconnect agreement.

The definitions of the other security terms used in this document can be found in [6].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CS2	Capability Set 2
CS3	Capability Set 3
CCF	Call Control Function
CCAF	Call Control Access Function
IN	Intelligent Network
IP	Intelligent Peripheral
INAP	Intelligent Network Application Part
ISUP	ISDN User Part
ITU	International Telecommunications Union
IWF	InterWorking Function
OS	Operation System
OSF	Operation System Function
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SMP	Service Management Point
SMAP	Service Management Access Point
SRF	Specialized Resource Function
SCEP	Service Creation Environment Point
SSF	Service Switching Function
SSCP	Service Switching Control Point
SS7	Signalling System number 7
TMN	Telecommunication Management Network

4 Introduction

As stated in the principles of Intelligent Network of ITU-T Recommendation Q.1201.

"The term Intelligent Network (IN) is used to describe an architectural concept which is intended to be applicable to all telecommunication networks. IN aims to ease the introduction of new services based on a greater flexibility and new capacities".

With the introduction of Capability set 2 (CS2) which permits interconnection of IN networks, proprietary security solutions are not sufficient due to the lack of interoperability. Moreover the definition of interfaces for interworking between IN-structured networks require new security solutions. Compared to the single network problem the security issues are changed and made more demanding.

These objectives require an adequate level of security to meet the requirements specified in [1].

A threat analysis according to the principles established by TC Security in [5] is therefore needed. Such a threat analysis is the main goal of the present document.

5 Security requirements for interconnected networks, as derived from business requirements

ETR 339 [1] lists business requirements and security aspects as seen from the objectives of customers, operators, economic entities and legislative entities. Security requirements applicable to the IN interfaces between functional entities have been extracted from the business requirements and aggregated. The following high level security requirements, applicable to interconnected networks, were identified:

- availability and reliability of IN interconnections;
- confidentiality (related to certain service data and personal data);
- integrity of data (especially related to charging and billing information);
- accountability of service operations;
- quick recovery from security and integrity failures.

A successful implementation of the security objectives and the management of the mechanisms are also highly dependent on close co-operation and agreements between operators. Co-ordination of security policies is required.

6 System description

To analyse security problems for IN interconnect, the three following diagrams have been studied. These diagrams are based on reference model to be found in [2], [3] and [4].

6.1 Basic block diagram

Two networks A and B may use some bidirectional interconnection arrangement to carry the information flows between them. An intruder may try to attack this interconnection arrangement.

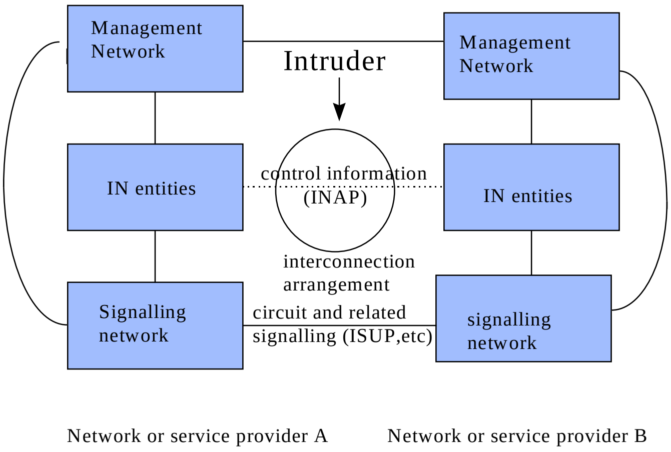
Management Network
Intruder
Management Network
IN entities
control information (INAP)
IN entities
interconnection arrangement
Signalling network
circuit and related signalling (ISUP,etc)
signalling network
Network or service provider A
Network or service provider B

Figure 1: Principle 7 networks interconnection

6.2 Block diagram at the functional level

When two networks communicate to each other, the system description at the functional level can be shown as follows:

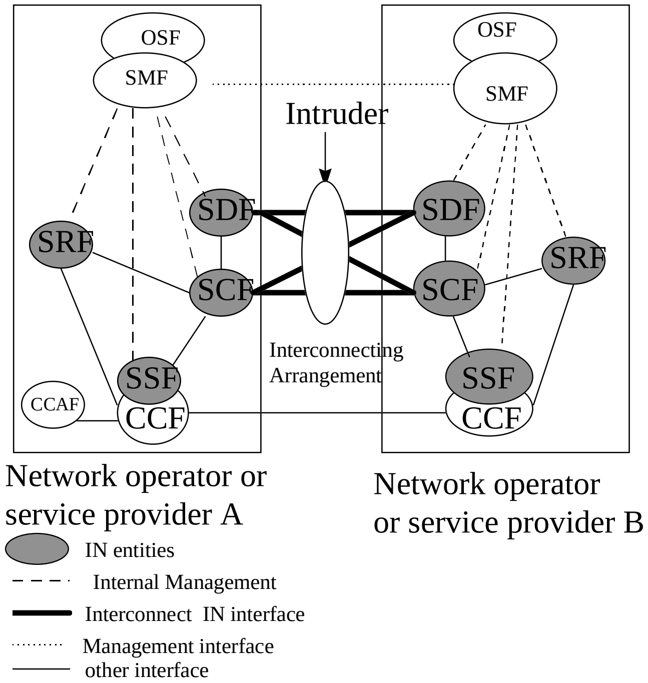
OSF
SMF
OSF
SMF
Intruder
SDF
SRF
SCF
SDF
SRF
SCF
SSF
CCF
CCAF
Interconnecting Arrangement
SSF
CCF
Network operator or service provider A
Network operator or service provider B
IN entities
Internal Management
Interconnect IN interface
Management interface
other interface

Figure 2: Functional level of network interconnection

NOTE : a) The OSF-OSF relates to the TMN.

b) A network operator or service provider need not employ all entities shown.

6.3 Block diagram at the physical level

When two networks communicate with each other, the system description at the physical level can be shown as follows:

The following diagram describes a possible physical representation, (all entities shown need not be used in a specific network).

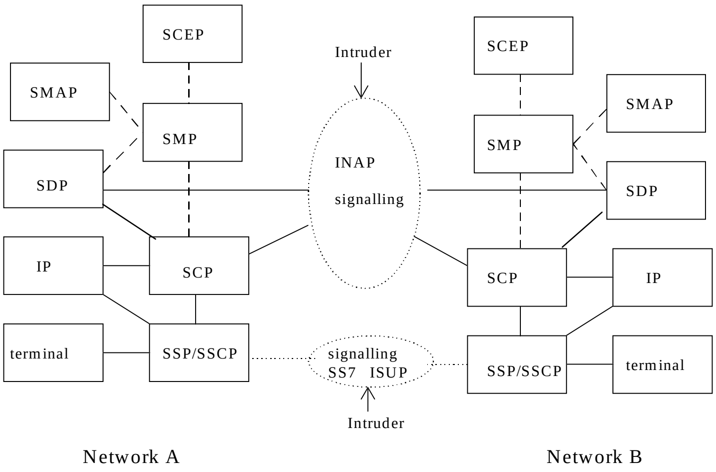

Figure 3: Physical level of network interconnection

7 Threat analysis

7.1 On vulnerabilities Threats and Intruders

The standardisation of the architecture concept of IN leads to a distribution of information (data, logic) over different entities defined in the distributed plane of IN conceptual model.

This distribution introduces new vulnerabilities on the communication between entities. The vulnerabilities on communication are similar within networks and between networks but the threats and the way to reduce them are different.

Generally, between two systems linked by a communication medium, the vulnerabilities are sorted in different families:

- vulnerabilities on communication path;
- vulnerabilities of connected « applications » running on the systems;
- vulnerabilities in network layer implementation;
- vulnerabilities of the operating system used in the system;
- vulnerabilities due to historical, legislative and management constraints;
- vulnerabilities linked to imperfection and tolerance.

In the present document, only the first three families are analysed. In practical application the other vulnerabilities should be taken into account.

The principal threats considered are:

- masquerade (« spoofing »);
- unauthorized access;
- eavesdropping;
- loss of information;
- corruption of information;
- forgery;
- repudiation;
- denial of service;
- replay of information;
- unauthorized activity.

The above mentioned threats can be put into effect by different types of intruders. Such intruders can be separated in the following main categories:

- external intruders;
- intruders within an organisation (unfaithful servants);
- accidental intruders (for instance due to lack of technical knowledge).

The external intruders are likely to be motivated by the opportunity to gain something for their own purpose and/or cause problems for the organisation being attacked. Internal intruders are likely to have personal motives, or act as agents for other organisations.

The third category need not be a malicious intruder, but may act as one due to incompetent or careless behaviour. In the new liberalised environment, many new entrants without previous experience in telecommunications can be foreseen. Consequently, this area should also be addressed in a comprehensive threat analysis.

7.2 List of threats

In the following, the threats mentioned above are described, and possible attack methods are considered. The resulting impact is given. For information, some countermeasures are mentioned, however they will be studied in detail in a following document.

7.2.1 Masquerade (« spoofing »)

Description

Masquerade is the pretence of one entity to be a different entity. There are different forms of masquerade attacks such as an interleaving attack which is a masquerade which involves the use of information derived from one or more ongoing or previous authentication exchanges. In order to perform such an attack, the first step will typically consist in obtaining access data through some means and then using it to obtain irregular access.

Possible Attack Methods

- tapping onto a link when a genuine entity has already established an interconnecting session on that link;
- let one entity on the interconnecting link falsely take on the identity of an other entity which it may or may not otherwise legitimately represent.

Impact

- reduction in quality of service provided;
- loss of confidence in the system;
- reporting of spurious faults;
- the suppression of genuine fault reports;
- generation of false data;
- service being illegally obtained causing loss of privacy;
- denial of service to the genuine entity;
- loss of information which could degrade the quality of service provided, lead to incorrect fraud handling and lead to a loss of confidence in the system;
- loss of revenue;
- inability to prevent fraud;
- loss of confidentiality.

Possible countermeasures

- entity authentication;
- message authentication;
- access control to authentication data;
- encryption;
- physical protection.

7.2.2 Unauthorized access

Description

An attacker gains access to a system or application to which he/she does not have the required permission.

Possible Attack Methods

- exploiting system weaknesses;
- misconfiguring equipment;
- masquerading as an entity with higher access permission.

Impact

- loss of confidentiality;
- loss or corruption of information;
- forgery;
- denial of service;
- theft of service.

Possible countermeasures

- well defined access control;
- authentication;
- security policy;
- properly controlled configuration.

7.2.3 Eavesdropping

Description

Unauthorised listening in to communications, resulting in a breach of confidentiality.

Possible Attack Methods

- using protocol or routing tools to redirect traffic to another network;
- attaching a protocol analyser to any accessible link;
- use of a device for eavesdropping and compromising switches used for the communication;
- illegal use of lawful interception facilities.

Impact

- loss of confidentiality of customer data;
- loss or confidentiality of service information data;
- loss of confidentiality of managemant information;
- loss of confidentiality of charging information;

  loss of confidentiality of authentication data.

Possible Countermeasures

- encryption of transmitted information;
- access control to transmission medium;
- physical protection;
- specific network configuration to reduce vulnerabilities.

7.2.4 Loss of information

Description

The destruction of information which may be stored or in transit along a path of communication.

Possible Attack Methods

- incorrect routing and addressing of messages;
- introducing severe message delays;
- various forms of blocking or interruptions preventing access or communication;
- unauthorized deletion of data;
- system or equipment failures with subsequent loss of data.

Impact

As a result, different types of data may be lost e.g. protocol and handling information, service data (charging data, call records), customer data (profiles) and general system data. The robustness of the protocols and system implementation will decide to what extent the lost information can be recovered quickly via mechanisms such as retransmission, rerouting, back up etc. The impact on service operation will depend on what kind of data is lost, and whether this data can be recovered or not.

Some examples of possible consequences of losing sensitive information without instant recovery are:

- reduced reliability and QoS due to disruption of services;
- reduced availability due to denial of service;
- complete loss of service;
- reduced quality of statistics and surveillance data for management purposes;
- reduced security level due to disruption of security procedures (access control, authentication, logging etc.);
- reduced trust, reputation and market share;
- reduced income due to loss of charging records (if carried over IN interfaces).

Possible countermeasures

- secure access control;
- protection of addressing and routing labels;
- comprehensive data recovery features;
- sequence control of messages;
- checked acknowledgement of messages.

7.2.5 Corruption of Information

Description

The compromise of data integrity by unauthorized insertion, modification or reordering.

Possible attack methods

- modifying transmitted information;
- modifying stored information, e.g. by masquerading or bypassing access control.

Impact

- incorrect routing and addressing of messages;
- various forms of interruption preventing access or communication;
- unauthorized modification of information;
- denial of service;
- incorrect billing;
- loss of trust;
- loss of customers.

Possible Countermeasures

- secure numbering of messages in combination with message integrity checks;

- security alarming;
- secure access control;
- Message Authentication Code;
- digital signature.

7.2.6 Forgery

Description

An entity fabricates information and claims that such information was received from another entity or sent to another entity.

Possible Attack Methods

- Fraudulent charging by a network operator (resulting in charging of events that did not exist or the wrong amount) can occur. This malevolent network operator can be the originating network one of the transit networks or the destination network.
- A network operator can also fabricate false messages involving other entities and then claim that such requests were received from another entity or sent to another entity. The communicating network will have to deal with those requests without be paid for that later on.

Impact

- loss of revenue;
- loss of trust;
- technical breakdown;
- possible extra costs for the network operators and/or users.

Possible countermeasures

- strong agreements between operators, discouraging irregular behaviour;
- audit;
- mutually agreed security policies;
- authentication mechanisms;
- digital signature.

7.2.7 Repudiation

Description

One or more users involved in a communication deny participation, a critical threat for electronic financial transactions (billing) and electronic contractual agreements.

Possible attack methods

- denial of transmission;
- denial of receipt;
- denial of having accessed data in a database;
- denial of having modified data in a database.

Impact

- loss of revenue;
- loss of trust;
- loss of customers.

Possible countermeasures

- digital signature;
- cryptosystems using Trusted Third Party;
- independent audit;
- strong agreements between operators, discouraging irregular behaviour.

7.2.8 Denial of service

Description

An entity fails to deliver its service or prevents other entities from delivering their services.

Possible Attack Methods

- interfering with signalling;
- modifying stored information;
- deliberate congestion;
- removing resources from service;
- physical destruction of equipment;
- misconfiguration of a component;
- interfering with cryptosystems.

Impact

- inability to perform desired functions;
- service failure;
- degradation of service;
- loss of income;
- loss of reputation;
- loss of customers.

Possible countermeasures

- message authentication code;
- digital signature;
- physical protection;
- access control;
- security alarms;
- automatic event handling;
- event monitoring.

7.2.9 Replay of information

Description

The repetition of previously transmitted information. The intention may be to corrupt service, causing overload or disruption.

Possible Attack Methods

- replay with modification of security procedures (e.g sequence number change);
- replay of a message (protocol data, system data, user data, etc…).

Impact

- overload;
- overcharging;
- loss of revenue;
- loss of trust;
- loss of customers;
- corruption of service;
- denial of service;
- masquerade.

Possible countermeasures

- message authentication code in combination with sequence numbers and/or time stamps;
- digital signature;
- event monitoring.

7.2.10 Unauthorized activity

Description

An attacker performs activities for which he has no permission or which are in contradiction of an interconnect agreement.

Possible Attack Methods

- exploiting system weaknesses;
- misconfiguring equipment.

Impact

- false service;
- disruption of service;
- denial of service.

Possible countermeasures

- event monitoring;
- authorisation;
- security policy;

- configuration control.

7.3 Risk analysis

The following table gives an evaluation of the main attack scenarios identified .For each attack scenario the likelihood and the impact have been evaluated in order to get the risk assessment of the attack method according to the method described in [5].

For the risk assessment the occurrence likelihood of threats is estimated from low to high. The meaning of the likelihood estimation of a particular threat is explained as follows:

Table 1: Likelihood

L	Low	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.
M	Medium	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
H	High	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

The impact of a threat is also estimated from low to high. The meaning of the impact evaluation is explained as follows:

Table 2: Impact

L	for "low impact"	The concerned party is not harmed very strongly; the possible damage is low.
M	for "medium impact"	The threat addresses the interests of providers / subscribers and cannot be neglected.
H	for "high impact"	A basis of business is threatened and severe damage might occur in this context.

The risk assessment is derived from the likelihood and the impact according to table 3:

Table 3: Derivation of the risk assessment

Likelihood	Impact	Risk assessment
L	L	L
M	L	L
H	L	M
L	M	L
M	M	M
H	M	H
L	H	M
M	H	H
H	H	H

The risk assessment of a threat is then derived and estimated from low to high. The meaning of the risk assessment is explained as follows:

Table 4: Risk

L	for "minor risk"	Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats causing minor risks have no primary need for countermeasures.
M	for "major risk"	Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimised as soon as possible.
H	for "critical risk"	Critical risks arise, when the primary interests of the providers / subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks must be minimised with highest priority.

Table 5: Risk Assessment

	Attack scenario	Threat Reference	Motivation	Likelihood	Im-pact	Risk Assess ment
1	Masquerading as a SCP in order to reduce or disable network capabilities	7.2.1	sabotage, financial	L	H	M
2	Masquerading as a SDP	7.2.1	financial (number portability case), breach of confidence, sabotage	L	H	M
3	Masquerade as a SCP to pervert network service.	7.2.1	malice ; destroy reputation ; financial	L	H	M
4	Abuse of access privileges via an SCP or SDP against/to an SCP or SDP	7.2.2	financial, sabotage	M	H	H
5	Subversion of OSF (e.g. insider attack leading to control over IN entities)	7.2.2 7.2.6	financial, commercial, revenge, espionage, denial of service, masquerading	H	H	H
6	Eavesdropping on a SDP-SDP interconnection in order to get customer information	7.2.3	financial, gathering intelligence, Interesting information can be : location, authentication information, privacy, billing information, management information	M	H	H
7	Eavesdropping on an SCP-SDP relationship	7.2.3	financial ; commercial ; espionage; personal espionage ; breach of privacy	H	H	H
8	An SCP deletes/modifies information (user data, system data, charging data) in an SDP	7.2.4 7.2.5	destroy reputation ; financial. This could also happen accidentally	M	H	H
9	Generation, deletion or modification of charging information in transit (assuming that IN entities may be used for charging in future)	7.2.4 7.2.5	financial, destruction of reputation	H	H	H
10	Disruption of maintenance state by modification of transmitted data	7.2.5	sabotage, destruction of reputation	L	M	L
11	Disruption of the distribution of service logic from the SMP/OS towards an SCP or an IP	7.2.5	sabotage, destruction of reputation, commercial	M	H	H
12	Modification of routing information	7.2.5	commercial, espionage	M	H	H
13	An SCP delivers incorrect routing information	7.2.5 7.2.6	financial, commercial, destruction of reputation. This could also happen accidentally	M	H	H
14	An SCP sends wrong charging information to another network (assuming that IN entities may be used for charging in future)	7.2.6	financial This could also happen accidentally	M	H	H
15	Generation of false traffic for purposes of fraud a) to gather interconnect charges for premium rate service fraud other value added service fraud	7.2.6 7.2.9	financial, commercial	H	H	H
16	An operator denies that his SCP has sent or received charging information	7.2.7	financial, commercial	M	M	M
17	An SCP or SDP is made unavailable (e.g. by message flooding)	7.2.8	denial of service, sabotage destruction of reputation, denial of service obligation, commercial advantage. This could also happen accidentally	M	H	H
18	Running a rogue service by a network against an other network	7.2.10	financial, This could also happen accidentally	M	H	H

Table 6: Risk assessment evaluation

19	Data trawling against an SDF, within an SCP or SDP	7.2.10	financial, espionage (personal and commercial information), marketing intelligence	M	H	H

History

Document history		
V1.1.1	July 1998	Publication

ISBN 2-7437-2409-9
Dépôt légal : Juillet 1998