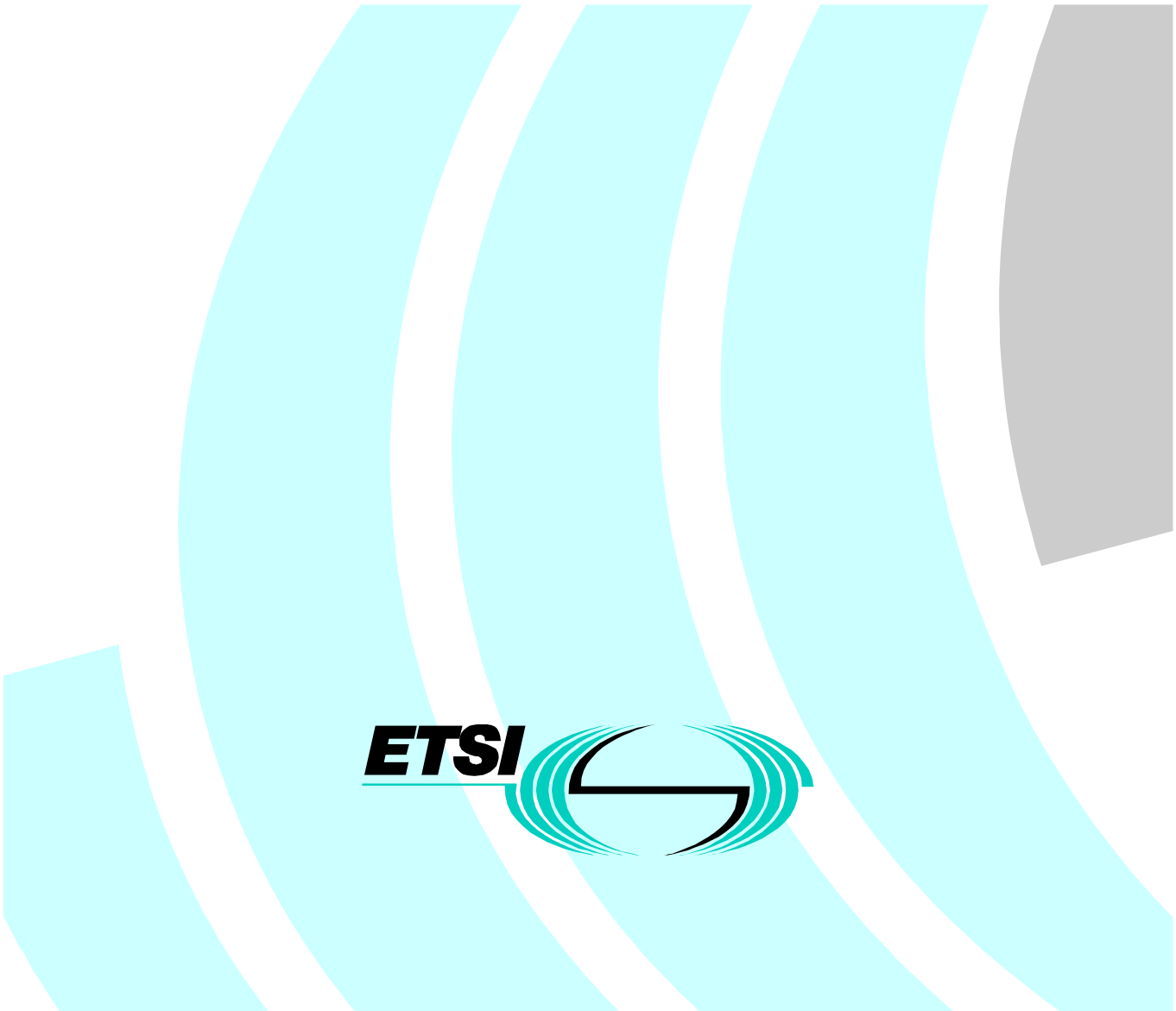
TR 101 664 V1.1.1 (1999-04)

Technical Report

Intelligent Network (IN); IN interconnect security features



Reference
DTR/NA-061205 (feo00ics.PDF)

Keywords
IN, security

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
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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

1 Scope

The present document describes security features which may be used in conjunction with the interconnection of two IN structured networks.

The purpose of the present document is to establish a set of technical requirements in order to meet the threats identified and analysed in a previous document. Those main threats due to IN interworking between IN structured network operators and/or service providers using CS2 and CS3 are listed in clause 5. IN CS4 will not be taken into consideration. The security implications of the use of the SCF-SSF interface for interconnection have not been studied in the present document. That interface is studied in detail in DTR/NA-061208.

The present document follows the successive steps:

- listing important threats;
- description of possible and existing security measures;
- discussion on which security measures to use in order to meet the threats.

The management aspects except those related to security policy are not included. They will be covered in EP TMN.

From the list of threat extracted from TR 101 365 [3], it is important to meet the most important ones in order to get a secure IN interworking. The aim of the present document is to select a good set of security features in order to build a security architecture for IN wich is described in TR 101 365 [3].

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 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

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

[3] TR 101 365: "Intelligent Network (IN); IN interconnect threat analysis".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

eavesdropping: breach of confidentiality by monitoring communication

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

replay of information: 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: entity fabricates information and claims that such information was received from another entity or sent to another entity

denial of service: prevention of authorized access to resources or the delaying of time critical operations

unauthorized activity: 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 the present document can be found in ETR 232 [1].

3.2 Abbreviations

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

IN CS2	IN Capability Set 2
IN CS3	IN Capability Set 3
IN CS 4	IN Capability Set 4
IN	Intelligent Network
IP	Internet Protocol
OSF	Operation System Function
SCP	Service Control Point
SDP	Service Data Point
SMP	Service Management Point
TMN	Telecommunications Management Network

4 Ordered list of threats

The following table gives the main threats and their risk identified during the threat analysis (see TR 101 365 [3]). The threats identified with a high risk are listed first, then the threats identified with medium risk and last the threats identified with low risk. The reference column refers to the threat analysis document TR 101 365 [3].

Table 1

	Attack scenario	Threat Reference	Motivation	Likelihood	Impact	Risk Assessment
1	Abuse of access privileges via an SCP or SDP against/to an SCP or SDP	7.2.2	Financial, sabotage	M	H	H
2	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
3	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
4	Eavesdropping on an SCP - SDP relationship	7.2.3	Financial; commercial; espionage; personal espionage; breach of privacy	H	H	H
5	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
6	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
7	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
8	Modification of routing information	7.2.5	Commercial, espionage	M	H	H
9	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
10	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
11	Generation of false traffic for purposes of fraud 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
12	An SCP or SDP is made unavailable (e.g. by message flooding)	7.2.8	Denial of service, sabotage destruction of reputation, commercial advantage. This could also happen accidentally	M	H	H
13	Running a rogue service by a network against an other network	7.2.10	Financial, This could also happen accidentally	M	H	H
14	Data trawling against an SDF, within an SCP or SDP	7.2.10	Financial, espionage (personal and commercial information), marketing intelligence	M	H	H
15	Masquerading as a SCP in order to reduce or disable network capabilities	7.2.1	Sabotage, financial	L	H	M
16	Masquerading as a SDP	7.2.1	Financial (number portability case), breach of confidence, sabotage	L	H	M
17	Masquerade as a SCP to pervert network service	7.2.1	Malice; destroy reputation; financial	L	H	M
18	An operator denies that his SCP has sent or received charging information	7.2.7	Financial, commercial	M	M	M
19	Disruption of maintenance state by modification of transmitted data	7.2.5	Sabotage, destruction of reputation	L	M	L

The introduction of IN CS4 could lead to a set of possible new threats which have not been considered here.

5 Security Features

In this clause, possible efficient security measures are described in details. For each of them, some examples of attacks on the IN interconnecting interfaces shown in figure 1 are given.

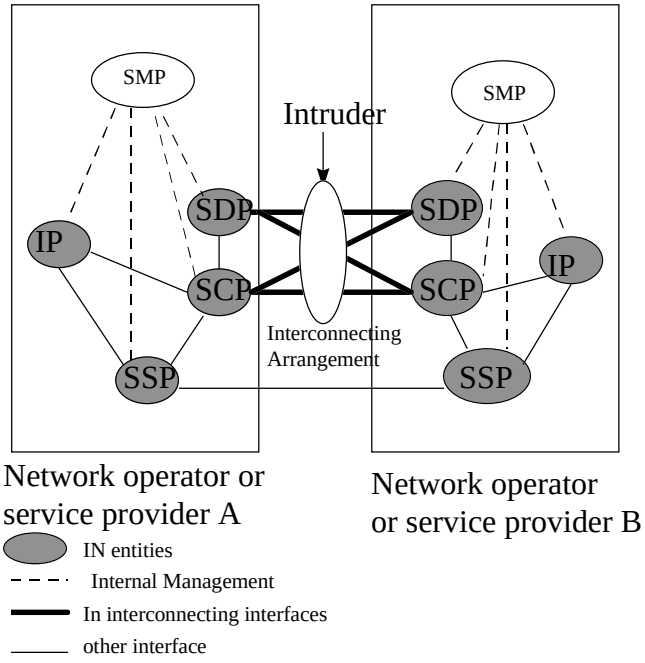


Figure 1: Physical representation

All the IN entities shown in the figure 1 should be physically protected.

5.1 Access control

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. Access control can be used to protect physical entities, software, data and the use of services. The SCP and the SCP require a particularly efficient access control system as they are the interworking identities (Attacks 1, 5, 6).

Access control to signalling data has not been considered here.

5.1.1 Access Control to Services

Prior to accessing IN services, an access control mechanism can check that the user has the access rights to use this service.

Access control to the IN service or to certain service functions can be seen as a combined process with identification and authentication of the involved parties, and subsequent authorization to use specified resources.

5.1.2 Access control to data

Users, other networks and differing members of the network operator's staff can access different part of the overall database. It is important to preserve the rights of access to each database. An access control mechanism may include authentication and can restrict access to parts of a database.

The access to service data can be restricted to the following subjects with different access rights:

- IN users/subscribers;
- management users (e. g. via internet);
- own IN entity;
- other network's IN entity.

The network operators have to restrict access to personal data in accordance to national (data protection) laws.

The IN network operator is responsible that only authorized personnel have access to the data.

Authentication data may need specific consideration.

5.1.3 Access control to software

The access to computers' operating software can be controlled. This is particularly important with respect to insertion of viruses. Authentication of personnel and access control in the IN systems may be provided.

5.1.4 Access control to hardware

Hardware can be protected against unauthorized actions either from the IN staff or intruders. Authentication of personnel and access control in the IN environment may be provided.

5.2 Authentication

Authentication is a property by which the correct identity of an entity or party is established with a required assurance. Authentication is possible for several purposes and between several entities.

5.2.1 Authentication between IN entities

Authentication (mutual or unilateral) of the IN entities (SCP and SDP in the interworking case as it is described in figure 1) can be provided for all request or command. The use of MAC can be a mechanism providing an implicit authentication. With a good authentication scheme, an SCP or SDP can be sure of the identity of the SCP or SDP interworking with it (Attacks 15, 16 and 17).

5.3 Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. It may be used to protect personal communications, personal data, and signalling data.

5.3.1 Confidentiality of data transmitted between IN entities

Security and other sensitive data such as session keys authentication data and personal data when sent between two networks can be protected by a number of mechanisms. Encryption is one such mechanism. It will be used to meet the threats 3 and 4.

5.3.2 Confidentiality of communications

Some communications could be very interesting for an intruder to eavesdrop. Message sent between two IN entities can be protected by a number of mechanisms. Encryption is one such mechanism.

5.3.3 Confidentiality of signalling

The occurrence of a communication may also need to be protected by confidentiality mechanism.

5.4 Data integrity

Integrity mechanisms ensure the prevention of unauthorized or accidental modification or deletion of information.

5.4.1 Transmitted data integrity

Data integrity mechanisms can be provided in the IN network for data transfers including: specified call forwarding number, call record data, billing records, messages between entities.

5.4.2 Stored data integrity

The update of data may be protected by use of relevant authentication and access control mechanisms. The service profile of each user for instance may be changed by an intruder or accidentally by the staff.

5.4.3 Data backup and recovery

To prevent loss of information due to unexpected events, regular backup of sensitive data may be performed.

5.5 Event and fraud monitoring

Recording and reporting the use of security services will allow the network operator to conduct security audits in order to detect actual threats against the IN system. Such audits may be used to investigate unauthorized change of database or abnormal patterns or misbehaviour or abuses.

The following data may be audited:

- use of the authentication mechanism
  (date, time, name of the network, success or failure of the authentication);
- attempted access to database
  (date, time, name of the attempting network, type of access attempt, success or failure of the attempt);
- actions by IN staff
  (date, time, name of the employee, type of action).

It should be possible to put both the security audit control mechanisms and resulting audit data into a number of categories. These categories could include:

- basic audit for fraud related purposes;
- audit for LI management;
- etc.

This would allow only authorized persons with specific access rights to obtain certain categories of security audits.

Dependent on the evaluation of audit data (on-line or off-line) some actions have to be carried out in order to enforce the security policy. These actions may include: alarms to the security administrator, or blocking of the subscription.

A good level of fraud control and event monitoring is necessary against the attacks which can be detected only after they have been performed (e. g. Threats 1, 9, 10, 11, 12, 13). It will be very important to take the appropriate measures as fast as possible to limit the impact of those threats.

5.6 Non repudiation

A non repudiation system is a system avoiding the denial of one entity involved in a communication of having participated in all or part of the communication. This kind of scheme is particularly useful regarding charging aspects. If some charging information are transmitted over the IN interworking interfaces such a scheme may be needed (Attack 18).

6 Analysis of threats & possible protection features

The following table gives the possible countermeasures to meet the list of threats identified as the main important ones in ETR 083 [2]. The threats are ordered from the most important ones to the less important one according to the risk assessment evaluated in ETR 083 [2]. Therefore the security measures meeting the first threats will be the basis of an IN security architecture offering a good level of security.

Table 2

Number	Threat description	Interface to be protected	Security feature
1	Abuse of access privileges via an SCP or SDP against/to an SCP or SDP	SCP - SCP SCP - SDP SDP - SDP	Access Control to data
2	Subversion of OSF (e.g. insider attack leading to control over IN entities)	All	Access Control to hardware/software
3	Eavesdropping on a SDP - SDP interconnection in order to get customer information	SDP - SDP	Confidentiality of data transmitted between IN entities
4	Eavesdropping on an SCP - SDP relationship	SCP - SDP	Confidentiality of data transmitted between IN entities
5	An SCP deletes/modifies information (user data, system data, charging data) in an SDP	SCP - SDP	stored data integrity access control to data
6	Generation, deletion or modification of charging information in transit (assuming that IN entities may be used for charging in future)	IN Interfaces used for charging if any.	Authentication Access control
7	Disruption of the distribution of service logic from the SMP/OS towards an SCP or an IP	All	Event and fraud monitoring
8	Modification of routing information	SCP - SCP	Transmitted data integrity
9	An SCP delivers incorrect routing information	SCP - SCP	Event monitoring
10	An SCP sends wrong charging information to another network (assuming that IN entities may be used for charging in future)	All	Event and fraud monitoring
11	Generation of false traffic for purposes of fraud: a) to gather interconnect charges for premium rate service fraud; b) other value added service fraud	All	Event and fraud monitoring
12	An SCP or SDP is made unavailable (e.g. by message flooding)	All	Event and fraud monitoring
13	Running a rogue service by a network against an other network	All	Event and fraud monitoring
14	Data trawling against an SDF, within an SCP or SDP	SCP - SDP SDP - SDP	Event monitoring
15	Masquerading as a SCP in order to reduce or disable network capabilities	SCP - SCP SCP - SDP	Authentication of SCP
16	Masquerading as a SDP	SCP - SCP SCP - SDP	Authentication of SDP
17	Masquerade as a SCP to pervert network service.	SCP - SCP SCP - SDP	Authentication of SCP
18	An operator denies that his SCP has sent or received charging information	SCP - SCP SCP - SDP	Non repudiation
19	Disruption of maintenance state by modification of transmitted data	SCP - SDP SDP - SDP	Transmitted data integrity

7 Conclusion

The security features described in clause 6 offer the capability to meet to some extent almost all the threats identified. The way to use them and to implement them is the subject of the next document. The security architecture for IN systems will mainly rely on those security features.

IN CS4 has not been considered during the threat analysis and therefore is not covered in the present document. Nevertheless IN CS4 will need further investigation.

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ETR 339: "Intelligent Network (IN); IN interconnect business requirements".
- ITU-T Recommendation Q.1221 (1997): "Introduction to Intelligent Network Capability Set 2".
- ITU-T Recommendation Q.1224 (1997): "Distributed functional plane for intelligent network Capability Set 2".
- ITU-T Recommendation Q.1228 (1997): "Interface Recommendation for intelligent network Capability Set 2".
- ITU-T Recommendation Q.1238 "Intelligent Network Interface Capability Set 3".
- ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".
- EG 201 620: "Intelligent Networks (IN); Security studies for Cordless Terminal Mobility (CTM)".
- DTR/NA-061208: "IN interconnect; Security of possible SCF-SSF or SDF-SSF interconnection between two or more networks".

History

Document history		
V1.1.1	April 1999	Publication

ISBN 2-7437-2999-6
Dépôt légal : Avril 1999