ETSI

ETSI TECHNICAL REPORT

ETR 339

March 1997

Source: ETSI TC-NA

Reference: DTR/NA-061203

ICS: 33.020

Key words: IN, interconnection, security

Intelligent Network (IN); IN interconnect business requirements

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

Introduction

This ETR is the first in a sequence of three ETRs and one ETS (European Technical Standard) which together consider the security of the Intelligent Network (IN) in relation to the interconnection of two or more networks employing IN technology.

Blank page

1 Scope

This ETSI Technical Report (ETR) describes the business requirements relating to the interconnection of two or more networks using Intelligent Network (IN) technology. These requirements relate to:

- customers;
- operators;
- economic entities;
- legislative entities.

NOTE: Within this ETR subscribers and users are referred as "customers" and network operators and service providers as "operators".

The need for security of internetworking is examined as well as general constraints such as performance and cost.

Intradomain (within a single network) security is out of scope of this document.

2 References

[1] ETR 301: "Users' Expectations; Virtual Private Networks".

3 Abbreviations

IN	Intelligent Network
ITSEC	Information Technology Security Evaluation Criteria
ONP	Open Network Provision
EII	European Information Infrastructure
GII	Global Information Infrastructure

4 General introduction

The goal of this ETR is to clarify the role of players, when it comes to interconnection of two or more networks using IN technology.

The Intelligent Network (IN) permits the improvement of existing services and the creation of new services. The modification and development of new services will be rapid. It will be easier to meet the expectations of customers than with pre-IN technology.

Operators will also seek improvement in the quality of the services offered, and reduction of the costs of network service operations and management.

Some of these services will require the interconnection of INs by their intelligence functions, rather than by the traditional circuit function. Modern services must be available across more than one network, and this report describes the security requirements from the point of view of several players who will be involved:

- customers, who receive services from the operators;
- operators, who provide networks and services;
- economic entities, who are concerned with economic efficiencies;
- legislative entities, who are concerned with legal issues, etc.

5 Business objectives and requirements

5.1 Customers' objectives

The requirements of customers are not uniform. For example, an enterprise does not always require the same as a private person. The following list is not exhaustive and is not priority sorted:

- availability of service;
- security:
  - functionality of service features:
    - data privacy;
    - confidentiality of service;
    - integrity of billing;
    - authorization and assured delivery;
    - the capability to use a service anonymously...;
  - assurance:
    - integrity of service operation;
    - quality of development and implementation;
    - probity of intervening parties;
  - no undesired consequences linked to the use of the service (e.g. burglary of a house because a feature provides information about the absence of its inhabitants);
- itemized and accurate billing;
- a low price;
- capability to use the service from "everywhere" or to be called from "everywhere";
- a tailored service to fit the exact need of users;
- management of some part of the service;
- user friendliness of the service;
- transparency to such changes as internal network modification, change of geographic area, change of service providers;
- capability to handle emergency calls:
  - carrying user's calls prior to any other features (authentication, screening) in order he could communicate with an emergency centre without delays;
  - avoiding an overload of emergency centres from malicious callers.

5.2 Operators' objectives

The principal business objectives of an operator may include:

- to attract and retain a large customer base;
- to offer services which customers want, quickly and efficiently;
- to generate revenue;
- to minimize costs;
- to operate at a competitive profit;
- to establish and protect a good reputation;
- to optimize the usage of resources (humans, computers, networks ...);
- to avoid the problems associated with breaches of security.

In order to attract and retain a large customer base, an operator could:

- offer a large number of services;
- offer services in a competitive way;
- offer services short time to market;
- offer wide geographic cover;
- offer attractive services (friendliness, security, fashion, functionality ...);
- offer a large interoperability with other IN services or networks.

Note that these business objectives and the possibilities listed above encourage an operator to interconnect with other operators to:

- offer wide geographic cover;
- offer services which can be achieved in no other way;
- complete each other offers in a new service;
- resell their services and network facilities to other operators;
- buy services and network facilities from other operators.

Both inside and outside its own network, an operator may be concerned for:

- performance;
- maximum re-use of existing systems;
- confidentiality;
- availability;
- accountability;

- security management functionalities (fraud management, trust management, integrity of exchanges ..);
- software assurance (quality level and Information Technology Security Evaluation Criteria (ITSEC) evaluation for example);
- network integrity;
- charging integrity;
- reliability;
- quick recovery of security or integrity failures;
- fault tolerance;
- management facilities;
- ease of the provision of new services with a short time to market.

5.3 Economic entities' objectives

Telecommunications takes a large part in economy as support or as product.

On these concerns, the economic parties may expect:

- a dynamic market with a fair competition between vendors and respect of client requirements;
- a good price of services and components;
- economic efficiency for manufacturers (standardization);
- a seamless web of Intelligent Networks which covers at least the European countries (European Information Infrastructure (EII)/Global Information Infrastructure (GII) concept);
- a permanent availability of this Web whatever the troubles (outage of one part, terrorism, strikes);
- a large offering of services whatever the place and the user;
- a secure provision of service (e.g. low rate of fraud).

5.4 Legislative entities' objectives

The IN and its use have to be in conformance with the different laws and regulations affecting telecommunications. These relate to:

- lawful interception;
- privacy rights:
  - data protection national acts, Europeans directives and International agreements;
  - confidentiality and telecommunication;
- intellectual rights;

- national laws (e.g. on cryptography);
- regulatory directives (e.g. Open Network Provision (ONP), number portability, spectral allocation);
- codes of practice;
- telecommunication licenses conditions;
- creation of a competitive market.

6 Security aspects

For IN technology to fulfil its promise of fast, efficient, low cost, rich services in a market environment, a widespread interconnection between networks is required. This interconnection will give rise to a number of risks which could be an hindrance to the objectives listed above.

6.1 Customer security

The effects on a customer of the network security hazards are:

- service unavailability;
- being charged for service not received;
- receipt of service from the incorrect operator;
- breaches of confidentiality and privacy;
- consequential impacts related to fraudulent activity.

6.2 Operator security

The impact of this interconnection on business is large. Indeed, an operator could face a large number of potential problems as a result of IN interconnection:

- network outages;
- computers failures;
- overload of its resources without compensation;
- overhead management costs;
- massive fraud;
- inability to trace calls;
- inability to get payment for a service
- inability to charge correctly;
- unfair competition.

And difficulties:

- processing and transport of confidential or sensitive information between interconnected domain;
- protection of confidential or sensitive information against an intruder third party;
- the provision of lawful interception for services provided across more than one domain;
- provision of decision points to arbitrate a case of dispute;
- evolution of IN structured network capabilities or change of network topologies with a difference space in each domain.

And consequences:

- loss of reputation;
- loss of business;
- forced abandonment of a market.

7 Conclusion

This ETR raises a number of potential threats that could be initiated when two or more networks are connected.

The threats analysis will describe how these risks could happen on network based on IN technology and the impact they could have.

When the technical solutions will be balanced, this ETR has to be kept in mind to be able to temperate the security choices with, for example, costs and performances. The security isn't a goal in itself.

History

Document history	
March 1997	First Edition

ISBN 2-7437-1355-0
Dépôt légal : Mars 1997