SLOVENSKI STANDARD
SIST-TP TR 101 771 V1.1.1:2004

01-april-2004

Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON), 4. izdaja - Definicija zahtev neodvisne storitve - Analiza groženj

Telecommunications and Internet protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent requirements definition; Threat Analysis

Ta slovenski standard je istoveten z: TR 101 771 Version 1.1.1

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TP TR 101 771 V1.1.1:2004 **en**

ETSI TR 101 771 V1.1.1 (2001-04)

Technical Report

TIPHON Release 4;
Service Independent requirements definition;
Threat Analysis

Reference
DTR/TIPHON-08002

Keywords
IP, network, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available 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 ETSI 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 Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1 Scope

The present document provides a comprehensive analysis of security threats to the TIPHON environment as described in principle in TS 101 313 [9]. It includes a definition of the security objectives, a description of the assets within the TIPHON environment, a list of threats to the TIPHON environment, a risk assessment, and a recommendation of the necessary security countermeasures.

TIPHON compliant systems bring together IP-based and SCN-based communications. Therefore it is recommended to comply with a certain level of security. Because of the well-known threats and counter-measures in the SCN, the present document focuses primarily on the IP-internal, IP-to-SCN functions.

The following network elements form the simplified TIPHON architecture as described in principle in TS 101 313 [9] for ITU-T Recommendation H.323 [12] to SCN interworking, which is used as basis for the present document:

- Terminals;
- Call control element, e.g. Gatekeeper;
- Admission control element, e.g. User Profile;
- Decomposed Inter-technology gateway consisting of:
  - Media Gateway Controller;
  - Media Gateway;
  - Signalling Gateway.

Where appropriate the guidelines for conduct of a threat analysis described in ETR 332 [1] are followed.

It is intended to expand the present document to cover additional functions and services in a future edition to cover the extended TIPHON environment described by TS 101 314 ed1 (for TIPHON release 2), for TS 101 314 ed2 (TIPHON release 3) and also in TS 101 882 [17] (TIPHON release 3) as an examination of threats against meta-protocols.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture".

[2] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[3] ETSI TR 101 750: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception".

[4] ITU-T Recommendation X.811 (1995): "Information technology - Open System Interconnection - Security framework for open systems: Authentication framework".

[5] ETSI ETR 237 (1996): "Security Techniques Advisory Group (STAG); Baseline security standards; Features and mechanisms".

[6] ETSI EN 301 261-3 (1998): "Telecommunications Management Network (TMN); Security; Part 3: Security services; Authentication of users and entities in a TMN environment".

[7] ISO/IEC 13335 (parts 1 to 5): "Information technology - Guidelines for the Management of IT Security (GMITS)".

[8] ISO/IEC 10181-4: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework".

[9] ETSI TS 101 313:"Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Phase II: Scenario 1 + Scenario 2".

[10] ISO/IEC 10181-3:"Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework".

[11] ETSI TS 101 323: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Interoperable security profiles".

[12] ITU-T Recommendation H.323: "Packet based multimedia communication systems".

[13] ITU-T Recommendation H.235: "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[14] ITU-T Recommendation H.245: "Control protocol for multimedia communication".

[15] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; TIPHON Release 2".

[16] RFC 2194 (1997): "Review of Roaming implementations".

[17] ETSI TR 101 882: "TIPHON Release 3; Protocol Framework Definition; General".

[18] RFC 2828: "Internet Security Glossary".

[19] RFC 2644: "Changing the Default for Directed Broadcasts in Routers".

[20] RFC 2267: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing ".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETR 232 [2] and the following apply.

NOTE: TIPHON is used in the following as synonym for "TIPHON compliant systems".

federation: collection of networked systems that can interact (interoperate) without being part of a single management domain

hijack attack: form of active wiretapping in which the attacker seizes control of a previously established communication association [18]

security policy: set of rules and practices that specify or regulate how a system or organization provides security to protect sensitive and critical system resources and the offered services

3.2 Abbreviations

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

BE	Back End
BER	Back End Routing function
CH	ClearingHouse
DoS	Denial of Service
GK	GateKeeper
GW	GateWay
ID	Identifier
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITSP	IP-Telephony Service Provider
MGC	Media Gateway Controller
MGW	Media Gateway
MMI	Man-Machine-Interface

NE	Network Element
OSP	Open Settlement Protocol
PIN	Personal Identification Number
PRS	Premium Rate Service
PSTN	Public Switched Telephony Network
RAS	Request Admission Status
RFC	Request For Comments
RS	Resolution Service
SAP	Service Access Point
SCN	Switched Circuit Network
SGW	Signalling Gateway
TCP	Transport Control Protocol
TIPHON	Telecommunication and Internet Protocol Harmonization over Networks
TR	Technical Report
UP	User Profile
UPT	Universal Personal Telecommunications
VoIP	Voice over IP

4 Overview

The present document follows the methodology generally described in ETR 332 [1] and is therefore structured in the following way.

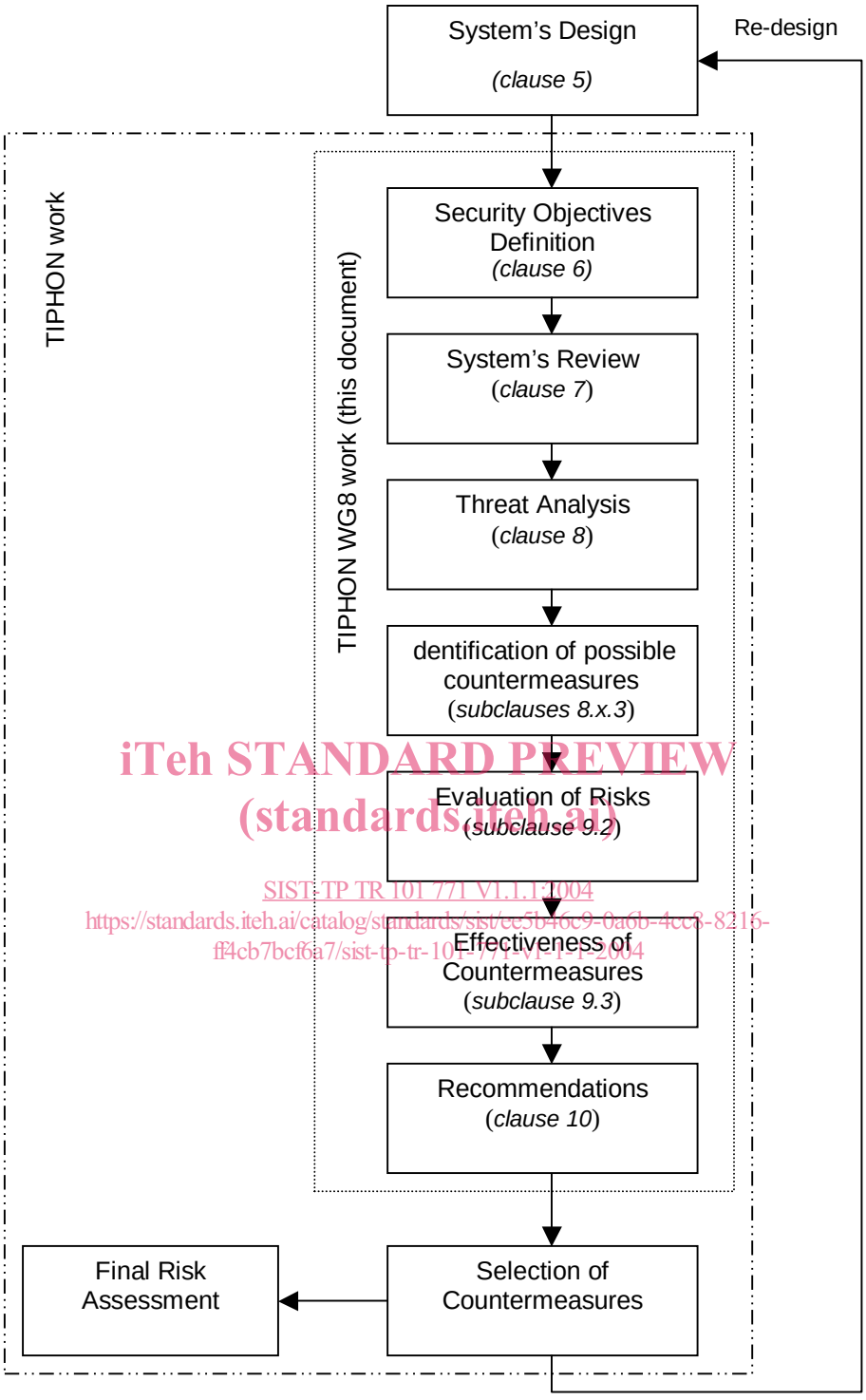

Figure 1: Structure of analysis

The present document is structured in the following way:

Clause 5 reflects the TIPHON architecture by using a simplified model as described in [17] according to the scope of the present document. The definition of the Security Objectives can be found in clause 6. A System's Review for a complete understanding of the system, its properties, boundaries and relationships to the external world is given in clause 7 based on a simplified architectural model. Clause 8 describes the threats identified to the network elements, their impact and lists possible countermeasures in clauses 8.1.3 to 8.7.3. The methodology of the risk assessment and the risk assessment itself is outlined in clause 9, covering the Evaluation of risks in clause 9.2 and the Effectiveness of countermeasures in clause 9.3. Clause 10 draws conclusions of the steps described in clauses 5 to 9 in listing a number of recommendations.

The following annexes are informative. Annex A deals with the Legislation Issues. Annex B provides a comprehensive description of the identified threats and gives examples. Annex C lists a number of countermeasures and possible implementations. Annex D contains a checklist for countermeasures against major threats.

5 System's Design

5.1 Network Architecture

This clause describes the general TIPHON network architecture in order to provide a basis to perform a complete threat analysis as outlined in clause 4. It covers the step "System's Review".

5.2 General Design

In this clause the mapping of the functional to the physical architecture and the network procedures are shortly described.

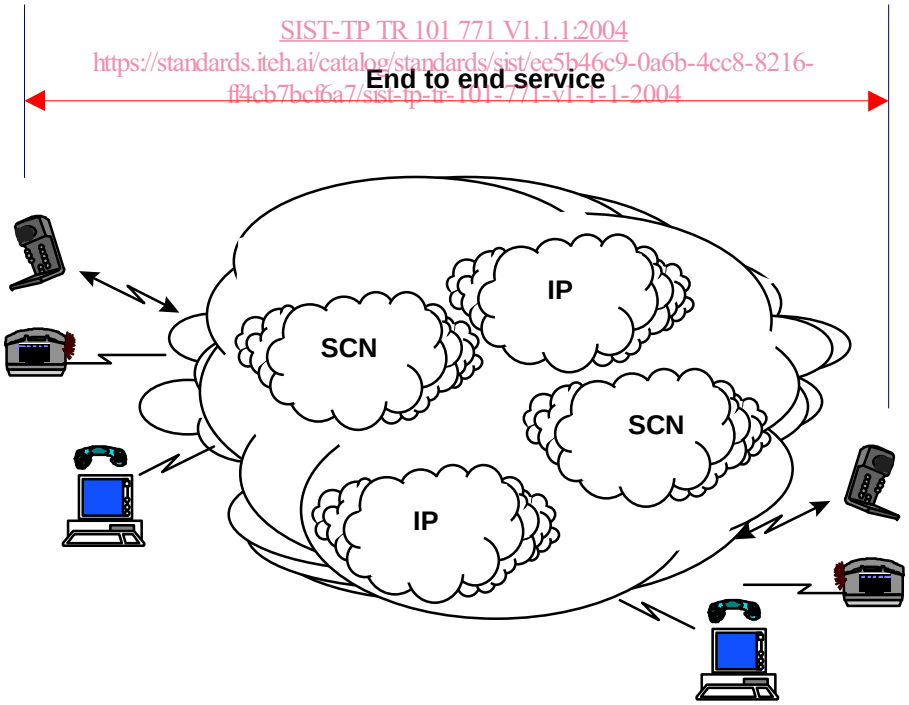

Figure 2: Overview of a general TIPHON domain

TIPHON can be drawn as a network of networks where the constituent networks may be based upon IP or Circuit Switching technologies. In addition TIPHON ensures that service users and providers are able to call upon standardized inter-domain settlement protocols.

The following assumptions shall apply as guiding principles for TIPHON:

- TIPHON terminals may be PC-like or telephone-like;
- the MMI of the terminal shall tend towards that of a telephone;
- operation of a TIPHON terminal shall tend towards that of a telephone (and shall therefore encompass single stage dialling, network type abstraction).

5.3 TIPHON Connectivity Scenarios

The TIPHON architecture is defined with respect to the support of a number of reference scenarios outlined below:

- the delivery of telephone calls which originate in an IP network and are delivered to Switched Circuit Networks (SCN), such as Public Switched Telephone Network (PSTN), Integrated Services Digital Networks (ISDN) and Global System for Mobile communication (GSM) networks (according to TIPHON Scenario 1);
- the delivery of telephone calls which originate in SCNs and are delivered in an IP network (according to TIPHON Scenario 2);
- the delivery of telephone calls which originate in SCNs, routed through an IP network and finally delivered to an SCN (according to TIPHON Scenario 3);
- the delivery of telephone calls which originate and terminate in IP networks. Such calls may be routed using an SCN (according to TIPHON Scenario 4).

NOTE: In each of the above cases the IP network hosted user is assumed to be using a TIPHON compliant terminal.

5.3.1 Scenario 1

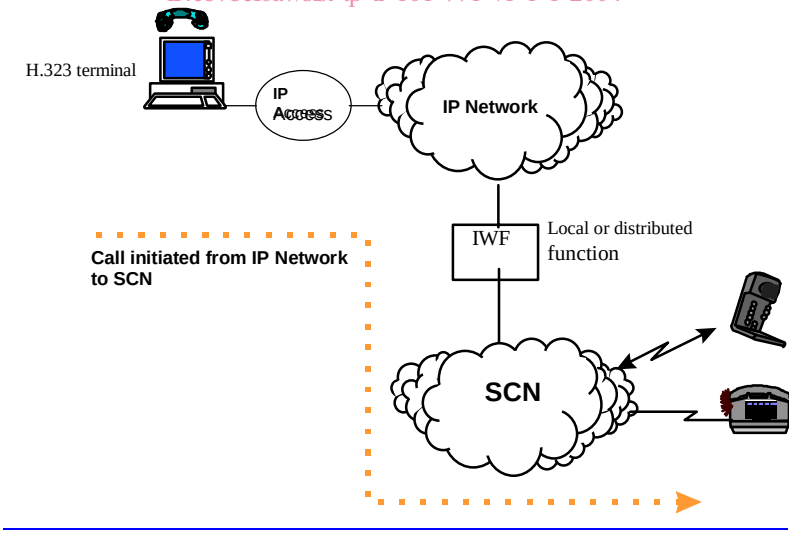

Figure 3: Scenario 1, Source on IP network to destination on SCN network

5.3.2 Scenario 2

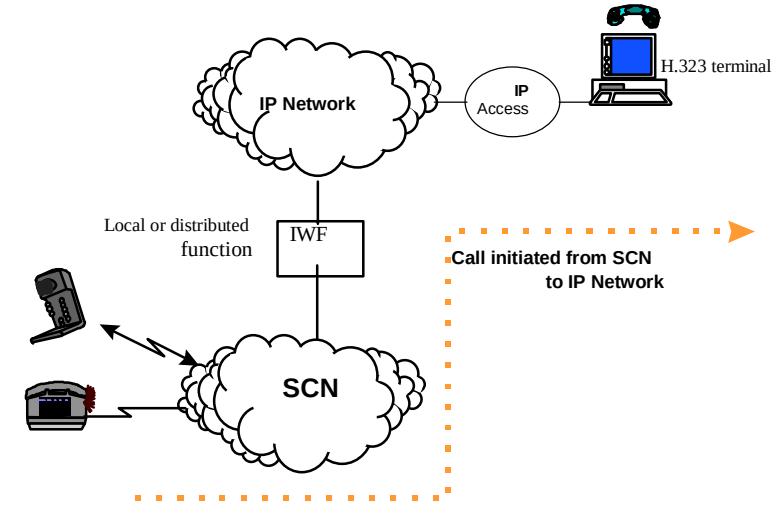

Figure 4: Scenario 2, Source on SCN network to destination on IP network

5.3.3 Scenario 3

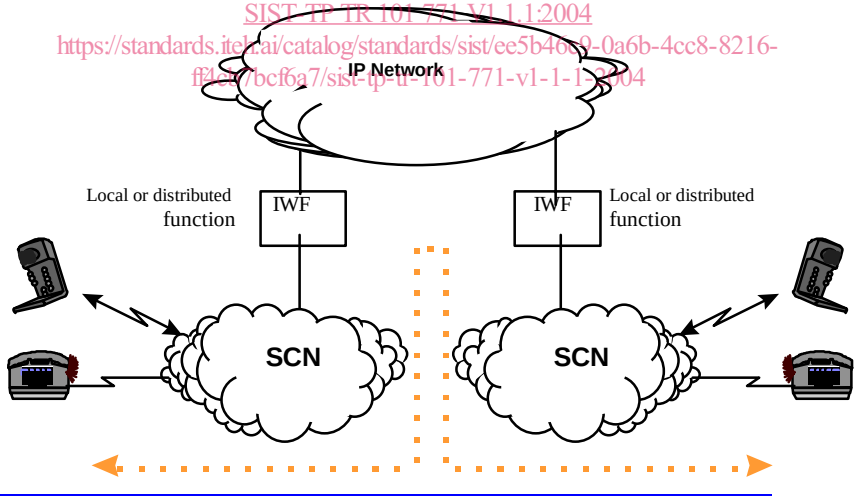

Figure 5: Scenario 3, Source and destination on SCN network using an IP transit network