SLOVENSKI STANDARD
SIST-TS TS 102 165-1 V4.1.1:2004

01-april-2004

Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON), 4. izdaja - Definicija okvira protokola - Varnostne metode in protokoli - 1. del: Analiza groženj

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis

Ta slovenski standard je istoveten z: **TS 102 165-1 Version 4.1.1**

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TS TS 102 165-1 V4.1.1:2004 **en**

ETSI TS 102 165-1 V4.1.1 (2003-02)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis

Reference
DTS/TIPHON-08005-1R4

Keywords
IP, protocol, security, VoIP

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://portal.etsi.org/tb/status/status.asp

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

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://webapp.etsi.org/IPR/home.asp).

All published ETSI deliverables shall include information which directs the reader to the above source of information.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

The present document is part 1 of a multi-part deliverable covering Methods and Protocols for security in TIPHON Release 4, as identified below:

Part 1: "Threat Analysis";

Part 2: "Counter Measures".

1 Scope

The present document defines by means of an information model, a functional entity behavioural model, and by validated SDL a model of the abstract behaviour of each service and service capability identified as being essential in TIPHON R4.

This part derives, by means of a threat analysis, the requirements for security features that when implemented are necessary and sufficient to ensure that TIPHON derived products do no harm to their participants.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] Void.

[2] ETSI TR 101 877: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Requirements Definition Study; Scope and Requirements for a Simple call".

[3] ETSI TS 101 878: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service Capability Definition; Service Capabilities for a simple call".

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[5] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[6] ETSI ETR 336: "Telecommunications Management Network (TMN); Introduction to standardizing security for TMN".

[7] ETSI TS 101 314: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Abstract Architecture and Reference Points Definition; Network Architecture and Reference Points".

[8] ETSI TS 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Part 1: Overview and Introduction".

[9] ETSI TS 102 165-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures".

[10] IETF RFC 3261: "SIP: Session Initiation Protocol ".

[11] ITU-T Recommendation H.323: "Packet-based multimedia communications systems".

[12] ITU-T Recommendation Q.1902 (1 to 6): "Bearer Independent Call Control protocol (Capability Set 2)".

[13] ETSI EN 300 347-1: "V interfaces at the digital Local Exchange (LE); V5.2 interface for the support of Access Network (AN); Part 1: V5.2 interface specification".

[14] IETF RFC 1889: "RTP: A Transport Protocol for Real-Time Applications".

[15] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

[16] IETF RFC 3015: "Megaco Protocol Version 1.0".

[17] IETF RFC 2327: "SDP: Session Description Protocol".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 101 877 [2] and TS 101 878 [3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations defined in TR 101 877 [2], TS 101 878 [3] and the following apply:

ATM	Asynchronous Transfer Mode
BICC	Bearer Independent Call Control
FDDI	Fibre Distributed Data Interface
GK	GateKeeper
GSTN	General Switched Talaphone Network
ISDN	Integrated Service Digital Network
LI	Lawful Interception
MEGACO	Media Gateway Control Protocol
NNI	Network to Network Interface
PBN	Packet Based Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RPC	Remote Procedure Call
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SASET	Secure Audio Simple Endpoint Type
SDP	Session Description Protocol
SET	Simple Endpoint Types
SIP	Session Initiation Protocol
SpoA	Service point of Attachment
SSCD	Secure Signature Creation Device
TpoA	Transport point of Attachement
TTP	Trusted Third Party
UAC	User Agent Client
UAS	User Agent Server

4 TIPHON overview

4.1 Introduction

TIPHON acts in the first instance as an umbrella set of service and service capability specifications defined in the form of a meta-protocol (see TS 101 882-1), and secondly as a set of protocol implementation mappings to the meta-protocol. In this respect there is no single protocol or service that has to be protected by counter measures within TIPHON. Furthermore the conventions of a threat analysis most often consider an implemented product (or protocol in TIPHON terms) and rarely deal with the purely abstract environment considered in TIPHON's meta-protocol.

4.2 Architecture

The TIPHON architecture shown in simplified form in figure 1 is formed from functional entities co-operating to provide capabilities which are then added to form services.

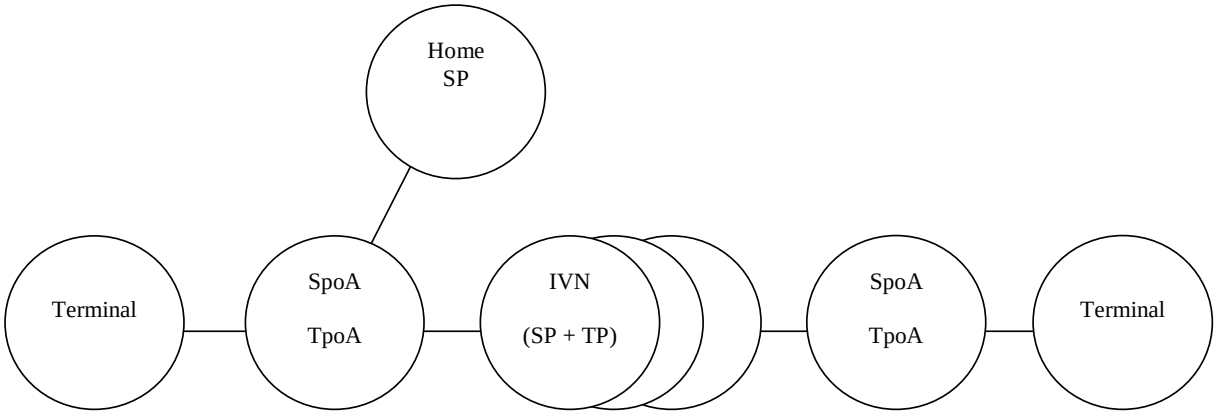

Figure 1: Simplified TIPHON interconnection architecture

In summary in TIPHON a Terminal is connected to a Serving network group that acts as both Service point of Attachment and as Transport point of Attachment (i.e. offers both service domain and transport domain). The serving network group is also connected to the Home Service Provider of the User and this acts as registrar and initial route for incoming calls. Between the originating and terminating domain may be one or more intervening domains containing both Service and Transport sub-domains.

The UNI interfaces have a scope of a single user. The Network to Network Interface (NNI) interfaces have a scope of many users.

Two forms of domain are considered in TIPHON: The Service Domain and the Transport Domain. The NNI signalling for a single service within the Service Domain may carry with it an association of many supporting services offered by the Transport Domain.

4.2.1 Specific meta-protocols

Each meta-protocol is described in terms of essential functional element and by identification of the information elements that need to be transferred between functional elements to facilitate operation. Threat analysis and countermeasures are in the first instance applied to the meta-protocol.

4.2.2 Specific implementations

Implementations that conform to the TIPHON meta-protocols are described for a number of protocol families and will include but not be restricted to:

SIP [10];

H.323 [11] (including H.225.0, H.245, H.248);

BICC [12]; and

V5.2 [13].

Where countermeasures exist in the meta-protocols to which a mapping is made then it is expected that a provision in the mapping for a specific protocol's implementation will also include provision of the countermeasures.

4.3 Forms of implementation

TIPHON, in achieving the goal of an umbrella specification, allows many forms of implementation. Each form of implementation will address a common set of threats, and will also address a technology specific set of threats. One of the goals of the present document (and its partner Countermeasures document) is to develop as large as possible the set of common threats and to therefore provide as large a set as possible of common countermeasures.

4.3.1 Terminal types

The user terminal for TIPHON services within the umbrella will fall within a continuum of implementations from hardware without built-in intelligence, to a wholly software platform with advanced intelligence. Examples are given in the following lists:

VoIP terminal types:

- Personal computer + SIP SW client;
- Personal computer + H.323 SW client;
- SIP HW telephone;
- H.323 HW telephone.

VoSCN terminal types:

- PSTN phone;
- ISDN phone;
- GSM terminal;
- 3G/UMTS terminal.

Hybrid terminal environments:

- PSTN/ISDN terminals connected directly to the PSTN/ISDN network;
- PSTN/ISDN terminals connected to an adapter for SIP telephony; and
- PSTN/ISDN terminals connected to an adapter for H.323 telephony.

4.4 Cryptographic countermeasures

Countermeasures to security threats do not need to be made cryptographic. In many cases countermeasures cannot be applied that employ cryptography. However where cryptographic countermeasures are employed they use essentially one of two (2) keying stratagems:

Symmetric keying

- Parties have access to the same key and generally only two parties are involved.

Asymmetric keying

- Each party has a two part key, one part is public and available to all correspondents, one part is private and known to only one party (the key owner). Security is derived from the premise that it is mathematically difficult (assumed impossible in current technology) to derive the private part from knowledge of the public part.

These keying mechanisms are generally bound to an identity and used to provide authenticity of the source, with the possibility to use the same keying stratagem for provision of confidentiality of transmitted content and for determining the integrity of transmitted content. Where the parties are known to one another in advance symmetric keying methods are traditionally favoured, and where the parties are unknown to one another in advance asymmetric methods are commonly employed.

Within the framework of TIPHON where a threat needs to be countered by the provision of cryptographic countermeasures both stratagems of keying should be supported.

4.5 Future TIPHON terminal

The constraints applied to future TIPHON terminals need to be considered.

The Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [4] quoted in the Official Journal L 013, 19/01/2000 P. 0012 - 0020 says:

QUOTE: Advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to hand-written signatures.

This may suggest that future TIPHON terminals take the form of a Secure Signature Creation Device (SSCD) and that standardizations must advance to a stage that a card can be inserted into any SSCD to enable authorization and authentication to services.

5 Security objectives

TIPHON™ shall meet the following objectives:

a) to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;

b) to ensure that the resources and services provided by serving and home functional groups are adequately protected against misuse or misappropriation;

c) to ensure that the security features standardized are compatible with world-wide availability (i.e. there should be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement, see bibliography);

d) to ensure that the security features are adequately standardized to ensure world-wide interoperability between different serving functional groups;

e) to ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services.

The basic security features employed in existing fixed and mobile systems will be retained, or where needed, enhanced. These include:

- subscriber authentication,
- encryption,
- subscriber identity confidentiality,
- use of removable subscriber module,
- secure application layer channel between subscriber module and home network,
- transparency of security features,
- minimized need for trust between home and serving functional groups.

The above objectives together can be met by provision of methods to achieve the following goals:

- **confidentiality**
  The avoidance of the disclosure of information without the permission of its owner.
- **integrity**
  The property that data has not been altered or destroyed in an unauthorized manner.

- **accountability**
  The principle whereby individuals are held responsible for the effect of any of their actions that might lead to a violation.

- **availability**
  The property of being accessible and usable upon demand by an authorized entity.

- **non-repudiation**
  A property by which one of the entities or parties in a communication cannot deny having participated in the whole or part of the communication.

6 Legislation issues

The following areas of legislation may have influence on the realization of security.

6.1 Privacy

Privacy legislation is of increasing importance; there are strong restrictions in many countries with regard to storage and visibility of data. Therefore, when offering a service within TIPHON, or when designing data processing functions and defining the kind of data being generated or stored within TIPHON systems, TIPHON service providers shall consider the relevant national data protection laws.

The definition of privacy includes:

- privacy of information: keeping information exchanged between service functions away from third parties;
- limitations on collection, storage and processing of personal data: personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of services;
- disclosure: the obligation of a network and service providers to keep information concerning customers away from third parties;
- inspection and correction: the right of the customer to inspect and correct information about himself stored by the service and/or network provider.

Privacy legislation will mostly concern the security objectives regarding "data confidentiality" and "data integrity". For TIPHON special concern in this respect shall be paid to the contents of personal data in the TIPHON service profile. These data and the access conditions to it for the service provider's personnel, the subscriber and the user himself shall be limited, in accordance with the relevant European guidelines and national laws.

6.2 Security order

National laws concerning the security order:

- demand proper protection of information and infrastructure to ensure the availability and the integrity of the telecommunication network;
- may restrict the usage of cryptographic methods.

This legislation will mostly concern the security objectives regarding "data confidentiality", "data integrity" and "availability".

6.3 Lawful Interception (LI)

Lawful Interception means the obligation of the network operator to co-operate and provide information in case of criminal investigations (see e.g. TS 101 331 [5]).

This legislation will mostly influence the security objectives regarding "data confidentiality".

6.4 Contract

It shall be possible to use information concerning the contract for communication services between two entities in case of a dispute in a court of law.

This legislation will mostly influence the security objectives regarding "accountability" and "data integrity".

7 Security framework

7.1 General assumptions

The following general assumptions are made for the provision of security functions in TIPHON:

- The user to SpoA link is vulnerable;
- The user to Registrar link is vulnerable;
- Links from SpoA to other network resident entities in the same network are not vulnerable;
- Links from the registrar to SpoAs in different networks/domains are vulnerable;
- Links between service domains are vulnerable;
- Links between service domains and transport domains are vulnerable; and
- Links between transport domains are vulnerable.

7.2 Capabilities in framework

7.2.1 Network access security

7.2.1.1 User identity confidentiality

The following security features related to user identity confidentiality should be provided:

- **user identity confidentiality:** the property that the permanent user identity of a user to whom a service is delivered cannot be eavesdropped on the access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the access link.

To achieve these objectives, the user should normally be identified by a temporary identity by which he is known by the visited (serving) network. To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's true identity is protected (enciphered) on the access link.

7.2.1.2 Entity authentication

The following security features related to entity authentication should be provided:

- **user authentication:** the property that the serving network corroborates the identity of the user;
- **network entity authentication:** the property that the serving network corroborates the identity of entities that operate within the network;