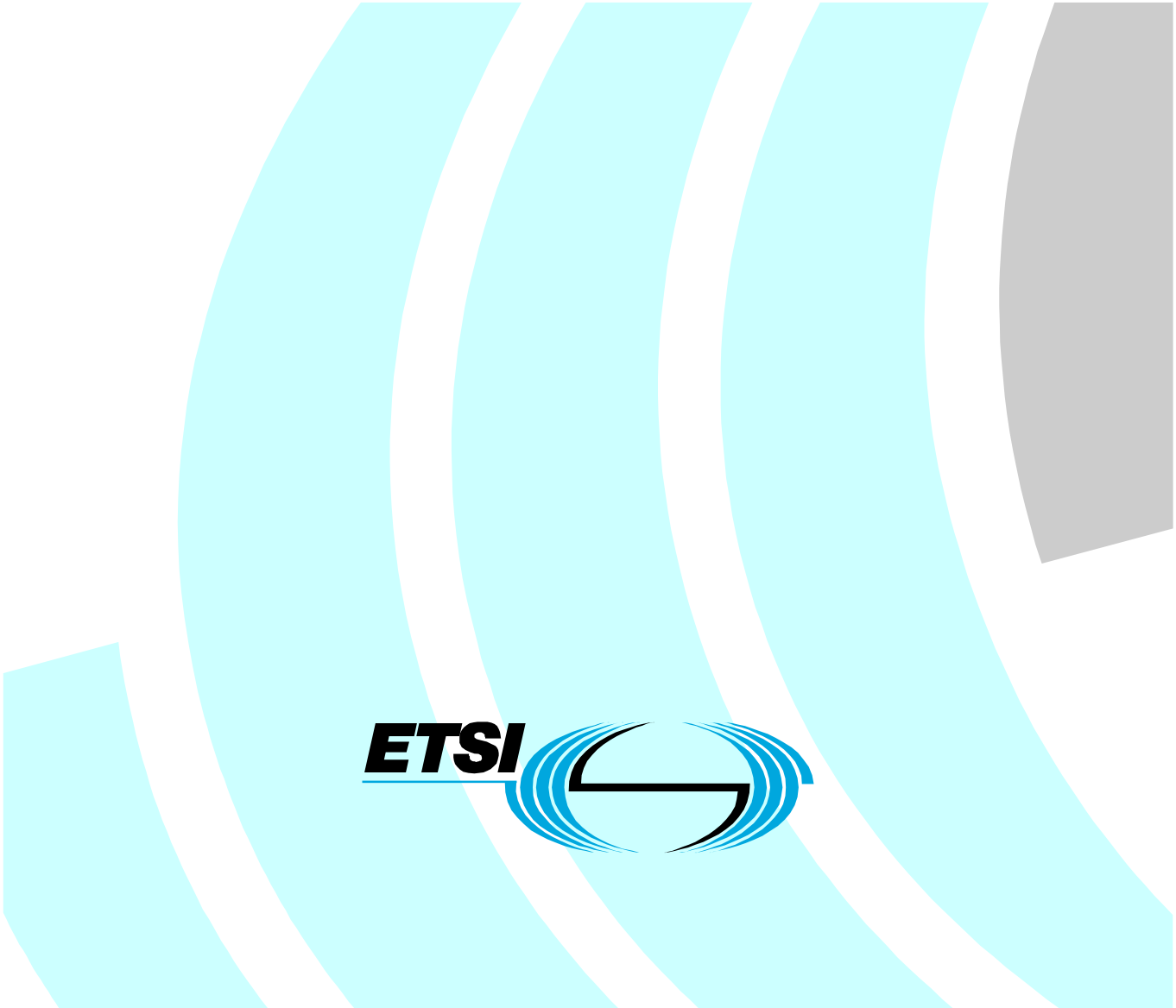
ETSI TS 102 165-1 V4.1.1 (2003-02)

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

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.

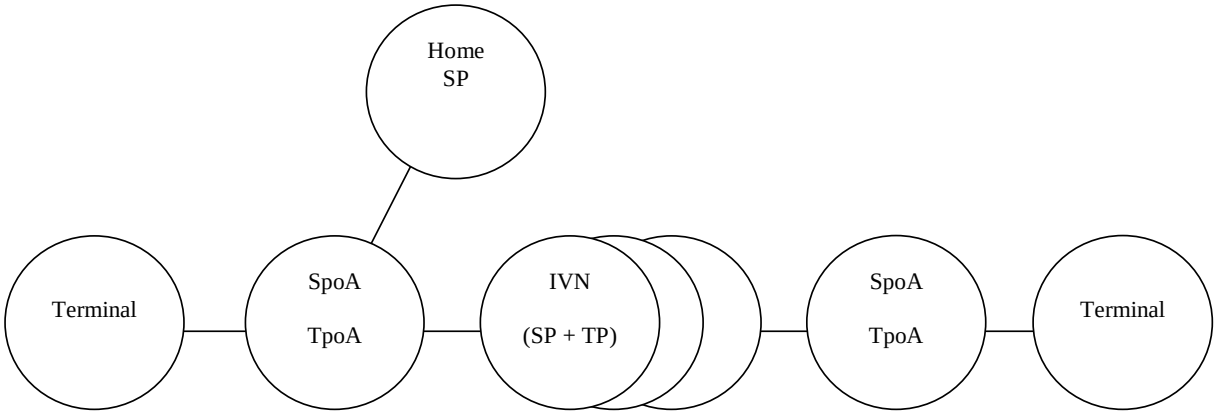


Figure 1: Simplified TIPHON interconnection architecture

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;

- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorized by the user's home to provide him services; this includes the guarantee that this authorization is recent.

7.2.1.3 Confidentiality

The following security features with respect to confidentiality of data on the access link (terminal to SpoA/TpoA) should be provided:

- **cipher algorithm agreement:** the property that the user and the SpoA can securely negotiate the algorithm that they shall use subsequently;
- **cipher key agreement:** the property that the user and the SpoA agree on a cipher key that they may use subsequently;
- **confidentiality of user data:** the property that user data cannot be overheard; and
- **confidentiality of signalling data:** the property that signalling data cannot be overheard.

Cipher key and cipher algorithm agreement should be realized in the course of the execution of the mechanism for authentication.

7.2.2 Security visibility and configurability

7.2.2.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the access link; and
- indication of the level of security: the property that the user is informed on the level of security that is provided by the SpoA.

7.2.2.2 Configurability

Configurability is the property that that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:

- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network; and
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

8 Threat analysis and risk assessment

8.1 Threats

In this clause a description of main threats concerning the network procedure aspects of TIPHON and the Management aspects is given, in order to evaluate risks. In the context of this concept paper, only intentional non-physical threats are taken into account. The following threats are partly derived from ETR 336 [6]. These threats are:

- 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 accesses data in violation to the security policy in force.

- Eavesdropping:

  A breach of confidentiality by unauthorized monitoring of communication.

- Loss or corruption of information:

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

- Repudiation:

  An entity involved in a communication exchange subsequently denies the fact.

- Forgery:

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

- Denial of service:

  An entity fails to perform its function or prevents other entities from performing their functions.

These threats counteract the identified main objectives as shown in table 1.

Table 1: Threats to security objectives

Threat	Objective			
	Confidentiality	**Integrity**	**Accountability**	**Availability**
Masquerade	X	X	X	X
Unauthorized access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of service				X

In a TIPHON context as defined in TS 101 882-1 call processing for normal priority calls against a TIPHON-id cannot be made prior to registration. It is a strong recommendation of TS 101 882-1 that registration of TIPHON-ids and attachment to an SpoA is performed on the basis of strong authentication (the methods for which are covered in TS 102 165-2 [9]).

8.2 Actors and roles

For the purpose of TIPHON security standardization, only technical security countermeasures are considered, which means that relevant actors to consider are *TIPHON users*. A TIPHON user is defined as a person or process using TIPHON in order to gain access to some TIPHON service. TIPHON users can further be categorized dependent on whether they belong to the organization running the TIPHON services (internal users) or whether they access the TIPHON services as external users.

Each time a TIPHON user accesses a TIPHON service, the TIPHON user will take on a role. In some cases there will be a one-to-one relationship between a TIPHON user and a role, i.e. the TIPHON user will always stay in the same role. In other cases there will be a one-to-many relationship between a specific TIPHON user and the possible roles the TIPHON user can play. This latter case is the normal TIPHON case in which the same user may act as a call initiator, call receiver, registrant, etc.

The following gives a high level classification of the most common roles:

- network operators (*private or public*);
- service providers (Bearer Service Providers or Value Added Service Providers);
- service subscribers/service customers;
- service end users;
- equipment/software vendors.

Some security measures may require actors to enforce the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with TIPHON.

8.3 Security domains

A *security domain* is defined as a set of entities and parties that is subject to a single security policy and a single security administration. A security domain may encompass many functional domains as defined in TS 101 314 [7].

8.4 Description of threats

8.4.1 General threats

8.4.1.1 Eavesdropping of TIPHON-id on interfaces or entities

It may be possible to eavesdrop a valid TIPHON-id. This could lead to other persons knowing the location of the TIPHON user, or to a masquerading threat (see also threats related to masquerading).

Resulting threats:

a) masquerading as a real user;

b) eavesdropping of personal information; and

c) communications pattern analysis (i.e. determining the forms of service invoked by a user and from that establishing the behaviour of the user to attack the privacy of the user).

8.4.1.2 Getting the TIPHON-id from a terminal

This could lead to other persons knowing the location of the TIPHON user, or to a masquerading threat (see later on threats related to masquerading).

Resulting threats:

a) masquerading as a real user;

b) eavesdropping of personal information; and

c) communications pattern analysis (i.e. determining the forms of service invoked by a user and from that establishing the behaviour of the user to attack the privacy of the user).

8.4.1.3 Denial of service

An attacker may wish to make any procedure impossible. This can be done at any interface used during the procedures (e.g. by modification of data) or by manipulating any entity used during the procedures. Normal service for the users and/or service providers is degraded or impossible.

Resulting threats:

a) denial of service;

b) degradation of service.

8.4.1.4 Unauthorized access to data

An attacker may wish to get some information stored in the databases.

Resulting threats:

a) denial of service;

b) masquerading as a real user;

c) eavesdropping of personal information.

8.4.1.5 Flooding the network

A motivation may be revenge or just hacking for fun. Any entities or interfaces can be the target for such an attack method.

Resulting threats:

a) denial of service;

b) degradation of service.

8.4.1.6 Stolen terminals

A stolen terminal can be used at least until the real user reports the theft of his terminal if the access to the terminal is not protected.

Resulting threats:

a) theft of service;

b) deciphering of previously recorded communications;

c) the attacker can receive incoming calls intended for the regular subscriber (in most cases for voice calls speaker recognition and/or the content of the conversation will identify such calls).

8.4.1.7 Subscription fraud

An attacker can take a subscription and use it extensively with no intention to pay (false address given, no money on his account, etc.).

Resulting threat:

a) loss of revenue.

8.4.1.8 Unauthorized access to data in terminals

An attacker may get some data from a terminal (e.g. TIPHON-id and authentication data) and use them later on.

Resulting threats:

a) masquerading;

b) deciphering of previously recorded communications.

8.4.1.9 Masquerading as one network entity to an other one

An attacker may try to masquerade as a network entity towards a network entity in order either to get information, pervert a service, deny a service or re-route some calls.

Resulting threats:

a) masquerade;

b) unauthorized access;

c) eavesdropping; and

d) denial of service.

8.4.2 Threats related to data deletion procedures

8.4.2.1 Eavesdropping of old address

An attacker may wish to trace the physical location of the user.

Resulting threat:

a) Knowledge of where a terminal was.

8.4.2.2 Masquerading as a network entity to delete data

An attacker may wish to delete records of the activity or of the presence of a user.

Resulting threat:

a) Incoming calls to a terminal may not happen; and

b) Records required for billing may not be available.

8.4.3 Threats related to subscription registration procedures

8.4.3.1 Illegal registration by an attacker masquerading as service provider

An attacker may wish to register a user with the intent of masquerade or to deny service to the legitimate user.

Resulting threat:

a) illegal registration leads to denial of service for the user; and

b) may be used as pre-requisite in a masquerade attack.

8.4.4 Threats related to subscription de-registration procedures

8.4.4.1 Illegal de-registration by an attacker masquerading as service provider

An attacker may wish to remove the registration of a user with the intent of masquerade or to deny service to the removed user.

Resulting threat:

a) illegal de-registration leads to denial of service for the user; and

b) may be used as pre-requisite in a masquerade attack.

8.4.4.2 Subscriber does not allow de-registration by manipulating his terminal

If the terminal is manipulated not to accept the network authentication which should accompany a withdrawal of the terminal's access rights, the user can inhibit the de-registration from taking effect in his terminal. Alternatively he can let the terminal send back a reject answer to the network's request, which indicates to the network that the re-register procedure has failed.

Resulting threat:

a) the attacker may be able to perform outgoing calls in a visited network, as long as authentication to the home network is not required.

8.4.4.3 Subscriber does not allow de-registration by manipulating the signalling interface

The attacker wishes to maintain service in the visited SpoA without knowledge of the registrar.

Resulting threat:

a) the attacker may be able to perform outgoing calls in a visited network.

8.4.5 Threats related to incoming call procedures

8.4.5.1 Masquerading by using someone's TIPHON-id

If authentication is not mandatory for incoming calls, a masquerading attack is possible by knowing only the TIPHON-id which can be caught easily (see general threats).

Resulting threats:

a) Incoming long distance calls will be (partly) billed to the regular subscriber in case of charging split. If the attacker gives the TIPHON number of that TIPHON subscriber to his friends, they can avoid high phone bills at the cost of the threatened subscriber.

b) The attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.

c) Duplication of TIPHON-id within inter-network. Both the attacker and the legitimate subscriber may attempt to register at the same time. The network cannot distinguish between a good and bad variant of the same TIPHON-id.

8.4.5.2 Masquerading by using someone's TIPHON-id and authentication information

Even if authentication and/or ciphering is required for incoming calls, a masquerading attack is possible by knowing the TIPHON-id and the authentication information which can be known by one of the methods described earlier.

Resulting threats:

a) Incoming long distance calls will be (partly) billed to the regular subscriber in case of charging split. If the attacker gives the TIPHON number of that TIPHON subscriber to his friends, they can avoid high phone bills at the cost of the threatened subscriber.

b) The attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.

c) Duplication of TIPHON-id within inter-network. Both the attacker and the legitimate subscriber may attempt to register at the same time. The network cannot distinguish between a good and bad variant of the same TIPHON-id.

8.4.5.3 Eavesdropping of the communication on the access interface by use of the session key

The attacker may have got the session key by one of the methods described earlier. He needs also be able to perform the cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher the intercepted communication.

8.4.5.4 Eavesdropping of the start of a communication on the access interface

This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started.

8.4.5.5 Eavesdropping of roaming number or routing number

This may occur at the SpoA entities of either the calling or called party.

Resulting threat:

a) this may lead to the knowledge of a TIPHON user's location.

8.4.5.6 Modification of routing data

The attacker may wish to modify the routing of calls to the benefit of one transit network over another, or to intercept calls.

Resulting threat:

a) The attacker may receive information intended for the regular subscriber. This threat is relevant especially for data services.

8.4.6 Threats related to outgoing call procedures

8.4.6.1 Masquerading by using someone's TIPHON-id

If authentication is not mandatory for outgoing calls, a masquerading attack is possible by knowing only the TIPHON-id which can be caught easily (see general threats). This attack is possible only if ciphering is not mandatory for exchanges between the SpoA and the terminal. Nevertheless even in that case the attacker may avoid ciphering by manipulating his terminal.

Resulting threat:

a) outgoing calls will be billed to the regular subscriber.

8.4.6.2 Masquerading by using someone's TIPHON-id and authentication information

Even if authentication and/or ciphering is required for outgoing calls, a masquerading attack is possible by knowing the TIPHON-id and the authentication information which can be known by one of the methods described earlier.

Resulting threats:

a) Outgoing calls will be billed to the regular subscriber.

8.4.6.3 Eavesdropping of the communication on the access interface by use of the session key

The attacker may have got the session key by one of the methods described earlier. He needs also be able to perform the cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher intercepted communication.

8.4.6.4 Eavesdropping of the communication on the NNI interfaces

Where ciphering is not performed eavesdropping can be done as in any fixed network.

8.4.6.5 Eavesdropping of the start of a communication on the access interface

This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started. Especially the called phone number and in case of specific services requiring, e.g. a PIN secret data may be eavesdropped.

8.4.6.6 Eavesdropping of the phone number of the called party

This may be possible since call set-up may start prior to authentication result and start of ciphering.

Resulting threat:

a) This may lead to the knowledge of a communication partner's identity.

8.4.6.7 Modification of the dialled number

In this attack the attacker intends to direct the communication to another address (which the attacker has access to).

Resulting threat:

a) The attacker may receive information intended for the TIPHON subscriber's communication partner. This threat is relevant especially for data services. Here it is not TIPHON specific.

8.4.6.8 Masquerading by using someone's TIPHON-id only

The attacker may with to avoid charging for a (probably short) period at the beginning of a communication

This may be possible since call set up may have been successfully performed before the authentication has been completed. This threat may especially be interesting in order to perform (short) calls to a premium rate service belonging to the attacker or his friends.

8.4.7 Threats related to emergency call procedures

8.4.7.1 Misuse of emergency call

An attacker can send some emergency calls e.g. to the police, without any reasons, e.g. to give false indications. In the case where giving the TIPHON-id without authentication is sufficient, he can masquerade as somebody else (if he knows his TIPHON-id). Then the emergency call seems to come from somebody else.

In TIPHON it is not necessary to have a TIPHON subscription for making emergency calls in a TIPHON compliant environment. Hence, an attacker can send some false indications when performing an emergency call, without giving any TIPHON-id. In that case, the misuse of emergency calls is even easier to perform.

NOTE 1: Emergency calls should be delivered with data identifying the location of the calling party.

NOTE 2: TIPHON provides a service level umbrella for the implementation of services in many candidate technologies. In extending that umbrella to cover SIM-enabled mobile devices it is understood that many of these devices are enabled to make emergency calls (i.e. those with service invocation code 112) when the SIM is removed from the device. When received by the network such calls are seen to be "identity-free".

Resulting threat:

a) masquerading and giving some false indication during emergency calls.

8.4.7.2 Manipulate data to give an emergency number to somebody

An attacker can give to a friend an emergency number by manipulating data in the emergency data base. In that case, this new number will be free of charge.

Resulting threat:

a) masquerading as an emergency entity, so that calls to this number are free of charge.

8.4.8 Threats related to service profile

8.4.8.1 Eavesdropping of transmitted information during service profile transfer

Resulting threat:

a) Personal data is divulged to unauthorized persons.

8.4.8.2 Manipulation of transmitted information during service profile transfer

Resulting threat:

a) The service is increased without authorization.

8.4.8.3 Unauthorized access to the service profile of somebody by unauthorized use of service profile interrogation

Resulting threat:

a) Personal data is divulged to unauthorized persons.

8.4.8.4 Unauthorized access to, or unauthorized use of, the service profile modification procedure

Resulting threats:

a) Modification of the service profile belonging to somebody else, e.g. in order to perform a denial or degradation of service.

b) Unauthorized modification of, e.g. one's own service profile, e.g. in order to increase the service without authorization.

8.5 Tabulated summary of threats

The following set of tables summarizes the threat descriptions given in clause 9.5.

Table 1a: General threats

Threats
8.4.1.1 Eavesdropping of TIPHON-id on interfaces or entities
8.4.1.2 Getting the TIPHON-id from a terminal
8.4.1.3 Denial of service
8.4.1.4 Unauthorized access to data
8.4.1.5 Flooding the network
8.4.1.6 Stolen terminals
8.4.1.7 Subscription fraud
8.4.1.8 Unauthorized access to data in terminals
8.4.1.9 Masquerading as one network entity to an other one

Table 2: Threats related to data deletion procedures

Threats
8.4.2.1 Eavesdropping of old address
8.4.2.2 Masquerading as a network entity to delete data

Table 3: Threats related to registration procedures

Threats
8.4.3.1 Illegal registration by an attacker masquerading as service provider

Table 4: Threats related to deregistration procedures

Threats
8.4.4.1 Illegal de-registration by an attacker masquerading as service provider
8.4.4.2 Subscriber does not allow de-registration by manipulating his terminal
8.4.4.3 Subscriber does not allow de-registration by manipulating the signalling interface

Table 5: Threats related to incoming call procedures

Threats
8.4.5.1 Masquerading by using someone's TIPHON-id
8.4.5.2 Masquerading by using someone's TIPHON-id and authentication information
8.4.5.3 Eavesdropping of the communication on the access interface by use of the session key
8.4.5.4 Eavesdropping of the start of a communication on the access interface
8.4.5.5 Eavesdropping of roaming number or routing number
8.4.5.6 Modification of routing data

Table 6: Threats related to outgoing call procedures

Threats
8.4.6.1 Masquerading by using someone's TIPHON-id
8.4.6.2 Masquerading by using someone's TIPHON-id and authentication information
8.4.6.3 Eavesdropping of the communication on the access interface by use of the session key
8.4.6.4 Eavesdropping of the communication on the NNI interfaces
8.4.6.5 Eavesdropping of the start of a communication on the access interface
8.4.6.6 Eavesdropping of the phone number of the called party
8.4.6.7 Modification of the dialled number
8.4.6.8 Masquerading by using someone's TIPHON-id only

Table 7: Threats related to emergency call procedures

Threats	
8.4.7.1	Misuse of emergency call
8.4.7.2	Manipulate data to give an emergency number to somebody

Table 8: Threats related to service profile procedures

Threats	
8.4.8.1	Eavesdropping of transmitted information during service profile transfer
8.4.8.2	Manipulation of transmitted information during service profile transfer
8.4.8.3	Unauthorized access to the service profile of somebody by unauthorized use of service profile interrogation
8.4.8.4	Unauthorized access to, or unauthorized use of, the service profile modification procedure

8.6 Risk Measurement

A potential threat is doing no harm unless there is a corresponding weakness in the system and until the point in time when a weakness is exploited by the intruder. Thus, the threats must be evaluated, i.e. it should be attempted to characterize them according to cost/effort involved (occurrence likelihood) and according to potential benefit/damage that can be done (impact value).

For the risk assessment, the occurrence likelihood of threats is estimated with values from "1" to "3". The meaning of a certain value associated to the occurrence likelihood of a particular threat is explained as follows:

Table 9: Occurrence likelihood

1	For "unlikely"	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.
2	For "possible"	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.
3	For "likely"	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 with values from "1" to "3". The meaning of a certain value associated to the impact is explained as follows:

Table 10: Impact

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

The product of occurrence likelihood and impact value gives the risk which serves as a measurement for the risk that the concerned management function is compromised. The result is classified into the following three categories:

Table 11: Risk

1, 2, 3	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 counter measures.
4	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 minimized as soon as possible.
6, 9	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 shall be minimized with highest priority.
NOTE: The values 5, 7, and 8 cannot occur.		

8.7 Risk Assessment for the TIPHON network procedures

General remark:

- All threats with risk 6 or 9 (critical risks) require countermeasures. Also threats with risk 4 (major risks) shall be minimized as soon as possible. The according security requirements are stated in clause 8.

Table 12: Risk assessment for general threats

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.1.1 Eavesdropping of TIPHON-id on interfaces or entities	3	2	6	Initial communication at any new TpoA/SpoA may have to receive the TIPHON-id in clear
8.4.1.2 Getting the TIPHON-id from a terminal	3	2	6	If the TIPHON-id is equivalent to a "telephone number" it may be visible from the terminal. If TIPHON-id is equivalent to the IMSI used in GSM/GPRS it should not be visible to the user (reduced occurrence likelihood).
8.4.1.3 Denial of service	3	3	9	
8.4.1.4 Unauthorized access to data	1	3	3	
8.4.1.5 Flooding the network	3	3	9	Developments in distributed denial of service attacks using legitimate transport protocols and remote invocation capabilities inherent in open processing platforms have made many attacks of this form simpler to invoke, and may be invoked transparently to the owner of the attack platform.
8.4.1.6 Stolen terminals	3	2	6	
8.4.1.7 Subscription fraud	3	2	6	Risk is greater for corporate rather than individual subscriber (many terminals versus single terminal).
8.4.1.8 Unauthorized access to data in terminals	1	3	3	
8.4.1.9 Masquerading as one network entity to an other one	2	3	6	Some technology devices (gateways) may be very straightforward to clone and to mount attacks from. In particular to manipulate call processing.

Table 13: Risk assessment for threats related to data deletion procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.2.1 Eavesdropping of old address	3	1	3	Minimize the risk by using non-global addressing. May require geographical address for location based services
8.4.2.2 Masquerading as a network entity to delete data	2	2	4	

Table 14: Risk assessment for threats related to subscription registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.3.1 Illegal registration by an attacker masquerading as service provider	2	2	4	Service dependent.

Table 15: Risk assessment for threats related to subscription de-registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.4.1 Illegal de-registration by an attacker masquerading as service provider	2	3	6	
8.4.4.2 Subscriber does not allow de-registration by manipulating his terminal	2	3	6	
8.4.4.3 Subscriber does not allow de-registration by manipulating the signalling interface	2	3	6	For user accessible application code such as SIP manipulation may be possible by use of virus infection.

Table 16: Risk assessment for threats related to TIPHON incoming call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.5.1 Masquerading by using someone's TIPHON-id	3	2	6	
8.4.5.2 Masquerading by using someone's TIPHON-id and authentication information	2	3	6	The design of the authentication mechanism should be sufficient to minimize the likelihood. If it is broken it will affect all on the network as the attack method may be reapplied.
8.4.5.3 Eavesdropping of the communication on the access interface by use of the session key	1	2	2	Session keys should not be exchanged in clear and have a lifetime very much less than the time required to determine the key.
8.4.5.4 Eavesdropping of the start of a communication on the access interface	2	2	4	
8.4.5.5 Eavesdropping of roaming number or routing number	2	2	4	
8.4.5.6 Modification of routing data	1	3	3	Routing data has commercial significance so will be highly protected.

Table 17: Risk Assessment for threats related to TIPHON outgoing call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.6.1 Masquerading by using someone's TIPHON-id	3	2	6	
8.4.6.2 Masquerading by using someone's TIPHON-id and authentication information	2	3	6	
8.4.6.3 Eavesdropping of the communication on the access interface by use of the session key	1	2	2	
8.4.6.4 Eavesdropping of the communication on the NNI interfaces	1	3	3	
8.4.6.5 Eavesdropping of the start of a communication on the access interface	3	2	6	
8.4.6.6 Eavesdropping of the phone number of the called party	3	2	6	
8.4.6.7 Modification of the dialled number	1	3	3	
8.4.6.8 Masquerading by using someone's TIPHON-id only	1	1	1	

Table 18: Risk Assessment for threats related to emergency call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.7.1 Misuse of emergency call	3	2	6	
8.4.7.2 Manipulate data to give an emergency number to somebody	2	3	6	

Table 19: Risk assessment for threats related to service profile

Threat	Occurrence Likelihood	Impact	Risk	Comment
8.4.8.1 Eavesdropping of transmitted information during service profile transfer	2	3	6	Service profile is probably easier to notice than other signalling as profile is a larger construct.
8.4.8.2 Manipulation of transmitted information during service profile transfer	1	3	3	
8.4.8.3 Unauthorized access to the service profile of somebody by unauthorized use of service profile interrogation	1	3	3	
8.4.8.4 Unauthorized access to, or unauthorized use of, the service profile modification procedure	1	3	3	

8.8 Consolidated Risk Assessment

Table 20 gives the identified **critical risks**, i.e. the risks with potential value 6 or 9.

Table 20: Threats with critical risk

Reference and Threat description
8.4.1.1 Eavesdropping of TIPHON-id on interfaces or entities
8.4.1.2 Getting the TIPHON-id from a terminal
8.4.1.3 Denial of service
8.4.1.5 Flooding the network
8.4.1.6 Stolen terminals
8.4.1.7 Subscription fraud
8.4.4.1 Illegal de-registration by an attacker masquerading as service provider
8.4.4.2 Subscriber does not allow de-registration by manipulating his terminal
8.4.4.3 Subscriber does not allow de-registration by manipulating the signalling interface
8.4.5.1 Masquerading by using someone's TIPHON-id
8.4.5.2 Masquerading by using someone's TIPHON-id and authentication information
8.4.6.1 Masquerading by using someone's TIPHON-id
8.4.6.2 Masquerading by using someone's TIPHON-id and authentication information
8.4.6.5 Eavesdropping of the start of a communication on the access interface
8.4.6.6 Eavesdropping of the phone number of the called party
8.4.7.1 Misuse of emergency call
8.4.7.2 Manipulate data to give an emergency number to somebody
8.4.8.1 Eavesdropping of transmitted information during service profile transfer
8.4.1.9 Masquerading as one network entity to an other one

Table 21 gives the identified major risks, i.e. the risks with potential value 4.

Table 21: Threats with major risk

Reference and Threat description
8.4.2.2 Masquerading as a network entity to delete data
8.4.5.4 Eavesdropping of the start of a communication on the access interface
8.4.5.5 Eavesdropping of roaming number or routing number
8.4.3.1 Illegal registration by an attacker masquerading as service provider

8.9 Conclusion

As a result of the previous risk assessment, we can conclude that the following groups of threat classifications are relevant for TIPHON and have to be carefully considered:

- Masquerading as a real subscriber in order to make calls without paying for them.

  The more often the attacker can perform this threat, the worse it is. To perform this threat, the attacker can manipulate the call forwarding service. For other attacks, the TIPHON-id of the real subscriber is needed. If authentication or ciphering is mandatory, authentication data or ciphering key is needed by the attacker. Several attacks can lead to getting this information:

  - in the distribution process procedure;
  - eavesdropping all of them during their transfer (over the air or in the network);
  - eavesdropping part of them during their transfer and guessing the rest of them by calculation;
  - masquerading as a network entity;
  - stealing a terminal and manipulating it; and
  - having unauthorized access to data in the network or in a terminal.

- Masquerading as a network entity to another one, e.g. as a false gateway:

  In the PSTN it has been difficult in general to masquerade as a network entity such as a switching centre. With the move towards soft switch and service platforms it is conceptually straightforward to launch masquerade attacks to perform secondary attacks as that network entity (c.f. above we declare this attack as a means of launching a subscriber masquerade). Such a masquerade can lead to billing fraud, obtaining information about the network, diversion of calls, DoS attacks.

- Eavesdropping of communications:

An attacker can perform this threat:

  - in the parts of the TIPHON network where encryption is not performed;
  - by masquerading as a network entity; and
  - by masquerading as the real subscriber and getting his incoming calls. To do this, the TIPHON-id is needed (see above for how to get the TIPHON-id), but the easiest way is to steal the targeted terminal. Another way is to manipulate the service profile or services such as call forwarding.

- Denial of service and degradation of service:

  This is possible against a service provider or a real subscriber.

  - It can be performed at any entity or interface;
  - One way to perform this threat is to have unauthorized access and manipulate the service profile or services such as call forwarding, incoming call screening, outgoing call barring;
  - Unauthorized generation of traffic on any of the TIPHON interfaces could lead to congestion in the network (flooding);
  - Abuse of emergency call may deny access to the emergency call centre for valid emergency notifications; and
  - Registering on a masqueraded TIPHON-id, leading to denial of service to the legitimate user.

- Billing fraud:

  Several kinds of billing fraud are possible:

  - subscription fraud leading to no payment of bills;
  - one network overcharges another network for roaming traffic; and
  - inhibit de-registration procedure in a visited network by manipulation of network entities, leading to no payment of calls.

- Other threats:

  Several kinds of other threats are possible:

  - unauthorized manipulation of incoming call screening or outgoing call barring, to make or receive calls that are not allowed (fraud of user against subscriber, e.g. his employer);
  - unauthorized access to data, to eavesdrop personal information; and
  - misuse of emergency calls via TIPHON can degrade or disturb the emergency call service.

9 TIPHON security requirements and security services

In the following, possible security requirements and security services to counter the critical and major risks are described. The tables at the end of this clause show the mapping of the identified threats to their countermeasures.

The general requirement is that countermeasures have to be taken against all threats evaluated with risk 4 or higher. These countermeasures cannot all be described at the same level of abstractness:

- some of them can be described as security services, placed at specified locations within TIPHON. The according security mechanisms will be specified in the next clause;
- some of them can be described as specific requirements on the use and specification of security mechanisms;
- some of them are more of a general nature giving guidelines for a security policy.

The security requirements and security services which will be defined in this clause are the following:

➨ **Authentication:**
- A1 = Authentication of the terminal by the registrar (home of the user profile);
- A2 = Authentication of the registrar by the terminal;
- A3 = Authentication of the terminal by the Service point of Attachment (SpoA);
- A4 = Authentication of the SpoA by the terminal;
- A5 = Authentication of the SpoA by the registrar;
- A6 = Authentication of the registrar by the SpoA;
- A7 = Authentication of the User to the TIPHON terminal device.

➨ **Access Control:**
- C1 = Access control to services;
- C2 = Access control to data;
- C3 = Access control to data in terminal;
- C4 = Access control to software;
- C5 = Access control to hardware.

➨ **Confidentiality:**
- E1 = Confidentiality of user communication on the access interface (terminal to TpoA);
- E2 = Confidentiality of signalling on the access interface (terminal to SpoA);
- E3 = Confidentiality of signalling between SpoA entities;
- E4 = Confidentiality of signalling between SpoA and TpoA;
- E5 = Confidentiality of communication between transport domains;
- E6 = Confidentiality of TIPHON-id on signalling interfaces;
- E7 = Confidentiality of communication between SpoA and Registrar (registration services)

➨ **Integrity:**
- I1 = Signalling data integrity;
- I2 = Bulk data transfer data integrity.

➨ **General Security Policy:**
- P1 = Bill limitations;
- P2 = Secure billing administration;
- P3 = Subscriber and terminal management;
- P4 = Hotline;
- P5 = Security related reports to the user;
- P6 = Secure dialogue between operators;
- P7 = Contractual agreements between operators;
- P8 = Contractual agreements between service providers and subscribers;
- P9 = Security related reports to the service providers;
- P10 = Secure subscription process.

9.1 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.

9.1.1 A1 = Authentication of the terminal by the registrar (home of the user profile)

The terminal shall contain a unique identity that identifies the registrar and authentication shall confirm this identity through proof of knowledge of a secret shared by the registrar and the terminal. This countermeasure is the corollary of A2.

9.1.2 A2 = Authentication of the registrar by the terminal

The terminal shall contain a unique identity that identifies the registrar and authentication shall confirm this identity through proof of knowledge of a secret shared by the registrar and the terminal. This countermeasure is the corollary of A1.

9.1.3 A3 = Authentication of the terminal by the Service point of Attachment (SpoA)

In order to offer service to the terminal the terminal shall be authenticated by the SpoA.

9.1.4 A4 = Authentication of the SpoA by the terminal

In order to validate that the SpoA is the one assigned by the registrar the terminal shall authenticate the SpoA.

9.1.5 A5 = Authentication of the SpoA by the registrar

The SpoA offering service to the registrant shall be authenticated to the registrar. This authentication shall be based upon secret data shared by the registrar and the SpoA. This countermeasure is the corollary of A6.

9.1.6 A6 = Authentication of the registrar by the SpoA

The registrar requesting service of the SpoA shall be authenticated to the SpoA. This authentication shall be based upon secret data shared by the registrar and the SpoA. This countermeasure is the corollary of A5.

9.1.7 A7 = Authentication of the user to the TIPHON terminal device

User authentication protects the terminal against misuse.

9.2 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.

9.2.1 C1 = Access control to services

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

Access control to the TIPHON 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.

9.2.2 C2 = Access control to data

Users, subscribers and the service provider's staff can access different part of the overall database. It is important to preserve the rights of access to each part of the 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:

- TIPHON user;
- TIPHON subscriber; and
- TIPHON service provider.

The service providers have to restrict access to personal data in accordance to national (data protection) laws. After termination of a subscription, the data may be deleted unless and only as long as they are required to deal with complaints, to recover charges or for legal obligations.

The TIPHON service provider is responsible that only authorized personnel have access to the data.

There may be a specific access control to the service profile data since some of these data may be changed on-line. The information stored in the service profile can be subdivided into fixed information and variable information from the TIPHON user's point of view. The fixed information is typically fixed at subscription time and can be changed only by the TIPHON service provider, possibly on request of the user. The variable information can be changed by the TIPHON user, by using TIPHON service profile management functions. Authentication data may need specific consideration.

9.2.3 C3 = Access control to data in terminal

A strong physical protection may be used for implementing the access control to the sensitive information stored in the terminal (e.g. keys, PIN). The use of the terminal may be controlled by authentication of the user (see also A7).

9.2.4 C4 = 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 service provider's systems may be provided.

9.2.5 C5 = Access control to hardware

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

9.3 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 and data, and signalling data.

9.3.1 E1 = Confidentiality of user communication on the access interface

Encryption on the access interface for outgoing and incoming calls, and for subscription registration procedure can provide confidentiality to the user communication and to TIPHON signalling.

9.3.2 E2 = Confidentiality of signalling on the access interface

The signalling can be protected on the access interface. Possible solutions include the use of encryption.

9.3.3 E3 = Confidentiality of signalling between SpoA entities

Security and other sensitive data such as session keys, call-forwarding number, and personal data can be protected by a number of mechanisms. Encryption is one such mechanism.

9.3.4 E4 = Confidentiality of signalling between SpoA and TpoA

The signalling interface between SpoA and TpoA may be protected. This may be done by physical protection or by cryptographic methods. Especially, the TIPHON-id and the session key may need to be protected.

9.3.5 E5 = Confidentiality of communication between TpoAs

The communication interface between TpoAs can be protected. This link may not be within a fixed network and therefore may be open to interception. This may be protected using either physical protection or encryption.

9.3.6 E6 = Confidentiality of TIPHON-id on signalling interfaces

The TIPHON-id can be protected on signalling interfaces. This may be protected by use of an alias-id or by encryption of signalling.

9.3.7 E7 = Confidentiality of communication between SpoA and Registrar (registration services)

NOTE: E7 may be considered as a special case of E2.

The link between SpoA and Registrar identifies the user of the service and may identify the key to be used in service E2.

9.4 Integrity

Integrity mechanisms ensure the prevention of unauthorized modification of information.

9.4.1 I1 = Signalling data integrity

Data integrity mechanisms can be provided in TIPHON for data transfers including: specified call forwarding number.

9.4.2 I2 = Bulk data transfer data integrity

Data integrity mechanisms can be provided in TIPHON for bulk data transfers including: call record data, billing records.

9.5 General security policy

Security policy forms part of the overall management structure of any network. Provisions for explicit security policy are therefore addressed in the network management documents of TIPHON [8].

A general security policy needs to be implemented to counter the identified threats. The following security requirements should be included within this policy.

9.5.1 P1 = Bill limitations

It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services.

Different methods, or combinations of methods, are possible to realize this requirement:

- Absolute bill limitation:

  When a subscriber opens an account, there can be an option to set a credit limit on the account. The total amount of the current bill of the subscriber may be checked at call set-up. A policy can be implemented about the acceptance or not of the call in case of exceeding bill limit. This can limit damage if abuse takes place.

- Bill limitation with respect to time:

  Another possible measure would be to limit the bill with respect to time. Thus, the credit limit may be on a day-by-day basis, on a weekly basis, or provide an overall limit. That means, if e.g. a limit per week is agreed and this limit is exceeded (at call set-up or during a call), the user access would be blocked for the rest of the week.

- Origin and Destination limits:

  Another security measure may be for certain accounts (for new or less trustworthy subscribers) to limit the destinations of calls. The limit may be within a given area, within the country, or even only to a specified destination address. Likewise, a limit may be put on the caller's location for outgoing calls.

9.5.2 P2 = Secure billing administration

The billing administration may have to consider security very carefully. Billing data and related personal data can be stored, processed, and transmitted in such a way that user privacy and data integrity are guaranteed. Itemized bills may be a means for the TIPHON subscriber to check the correctness of the billing. Thus, the billing administration can send to the user an explained bill with the called numbers and split in different part like regional calls, national calls, international calls. However, to avoid conflicts with privacy requirements, the subscriber can also have the possibility to get only summarized bills.

9.5.3 P3 = Subscriber and terminal management

Limiting the access to services by means of subscription restriction or equipment restriction can reduce otherwise unacceptable risks. This can be achieved in a number of ways such as by the use of black lists to identify rogue subscribers or rogue equipment. Service may be denied to subscribers or equipment that appears on such a black list.

A white list gives unrestricted access to subscribers and equipment (within any limits set by their service profile). Intermediate variants of these lists may be maintained to track potential bad debt or potential fraud.

9.5.4 P4 = Hotline

A Hotline can be provided by the operator in order to answer users' questions like " My service does not work", "I have received too high a bill". This service may be useful for security reasons in case of theft or loss of terminal or in case of unexpected behaviour of the service of a subscriber where specific procedures should be implemented. In case of theft or loss of terminal, this procedure can be:

- location of the stolen or lost terminal in order to find it;
- block incoming and outgoing calls;
- put the TIPHON number on a black list;
- no charging for the subscriber of calls performed after the report of the theft; and
- de-registration of the terminal after location.

9.5.5 P5 = Security related reports to the user

Recording and presentation of information about actions performed by users in the system (event reporting) may often function as a supporting security service. (Users' knowledge of this fact may in turn work as a deterrent factor). Announcements must be carefully designed to enlighten users and third parties of the different states of their connection or relation with the operator/service provider. There can be a facility to inform TIPHON users about actions that affect their privacy and security or the charging. This information can be given on-line by announcements, special dial tones, or short messages.

For example, the following information can be given to the users:

- "BILL LIMITATION EXCEEDED".

9.5.6 P6 = Secure dialogue between operators

Secure dialogues can consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link. It can be provided by:

- mutual authentication;
- link encryption;
- link data integrity;
- non-repudiation; and
- key management to support this.

9.5.7 P7 = Contractual agreements between operators

Contractual agreements relating to security issues can be included in the roaming agreement between two operators.

When agreeing upon a roaming agreement two operators may define some security conditions. Those conditions can be:

- frequency of exchange of blacklists;
- liability of a visited network if it does not take the appropriate measures to stop a fraud;
- level of security audit guaranteed;
- follow the rules concerning the use of data an other network can get access to;
- co-operation in case of fraud;
- integrity of file transfer;
- minimum frequency of authentication to be performed for visiting TIPHON users; and
- in case of dispute, one network operator should be able to provide the other network with every information related to billing.

9.5.8 P8 = Contractual agreements between service providers and subscribers

Contractual agreements relating to security issues shall be included in the conditions for the subscription. Security conditions to be agreed and signed by the subscriber could be:

- to follow the rules (as declared by the TIPHON service provider and adjoined to the subscription contract) regarding secure handling of his PIN if used to protect terminal;
- to report to the service provider immediately loss of terminal which might lead to fraud or misuse;
- to accept limitations of service with regard to agreed levels of credit control/bill limitation; and
- to accept limitations of service which the service provider later on may find necessary to introduce to protect the service as such against misuse or fraud.

9.5.9 P9 = Security related reports to the service provider

Recording and reporting the use of security services will allow the service provider to conduct security audits in order to detect actual threats against the TIPHON system. Such audits may be used to investigate unauthorized use of a TIPHON terminal or unauthorized change of profile or abnormal patterns or misbehaviour or abuses.

The following data may be audited:

- use of the authentication mechanism (date, time, TIPHON-id, location, number dialled, success or failure of the attempt);
- attempted access to the service profile (date, time, TIPHON-id, name of the object, type of access attempt, success or failure of the attempt); and
- actions by TIPHON service providers staff (date, time, TIPHON-id, type of action).

In practice the audit will be restricted to specific sets of users.

Access to audit data should only be permitted to authorized persons (see also C2, C4 and C5).

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.

9.5.10 P10 = Secure subscription process

A secure subscription process can restrict subscription fraud. A security policy may be applied to new subscribers in order to be to be confident in the ability and motivation of a subscriber to pay any bills. This may be achieved by authenticated or verified delivery of proofs of identity.

It may be possible for subscriptions to be made available on a pre-paid (contract less) basis. It can be possible to inhibit service when the pre-payment is exceeded.

The operator may restrict the number of subscriptions per subscriber.

9.6 Threats and counteracting security measures

As a first step in the process of selecting relevant and suitable security services for TIPHON, the following choices were made.

- A1 = Authentication of the terminal by the registrar (home of the user profile)
- A2 = Authentication of the registrar by the terminal
- A3 = Authentication of the terminal by the Service point of Attachment (SpoA)
- A4 = Authentication of the SpoA by the terminal
- A5 = Authentication of the SpoA by the registrar
- A6 = Authentication of the registrar by the SpoA
- C1 - C5 = Access control to services, to service data in databases, to data in terminals, and to the service provider's software and hardware, respectively;
- E1 = Confidentiality of user communication on the access interface;
- E2 = Confidentiality of signalling on the access interface;
- E3 = Confidentiality of signalling between SpoA entities;
- E6 = Confidentiality of TIPHON-id on signalling interfaces;
- E7 = Confidentiality of signalling between SpoA and Registrar;
- P1 = Bill limitations;
- P2 = Secure billing administration;
- P3 = Subscriber and terminal management;
- P9 = Security related reports to the service providers; and
- P10 = Secure subscription process.

These measures are a natural start for one, or several, of the following reasons:

1) These countermeasures will cover all threats with potential risk 9 and in addition many other threats.

2) They belong to a set of security policy decisions that are of such a generic nature that they can be expected to be inherently present in a public network service like TIPHON.

3) The mechanisms cover more than one communication event.

Table 22: Threats with potential risk 9 and 6 covered by initial selection of countermeasures

Reference and Threat description	Security Requirements and Services
8.4.1.1 Eavesdropping of TIPHON-id on interfaces or entities	E2; E3
8.4.1.2 Getting the TIPHON-id from a terminal	C3
8.4.1.3 Denial of service	P3; P10; A1; A2; C1
8.4.1.5 Flooding the network	C1
8.4.1.6 Stolen terminals	A7
8.4.1.7 Subscription fraud	A1; A2; C1
8.4.4.1 Illegal de-registration by an attacker masquerading as service provider	A1; A2; A5; A6; C1
8.4.4.2 Subscriber does not allow de-registration by manipulating his terminal	C3; C4; C5
8.4.4.3 Subscriber does not allow de-registration by manipulating the signalling interface	C3; C4; C5
8.4.5.1 Masquerading by using someone's TIPHON-id	A1; A2
8.4.5.2 Masquerading by using someone's TIPHON-id and authentication information	A7; A1; A2; E1; E2; E6
8.4.6.1 Masquerading by using someone's TIPHON-id	E1; E2; E6
8.4.6.2 Masquerading by using someone's TIPHON-id and authentication information	A7; A1; A2; E1; E2; E6
8.4.6.5 Eavesdropping of the start of a communication on the access interface	E1; E2; E6
8.4.6.6 Eavesdropping of the phone number of the called party	E2
8.4.7.1 Misuse of emergency call	C1
8.4.7.2 Manipulate data to give an emergency number to somebody	C1; C2
8.4.8.1 Eavesdropping of transmitted information during service profile transfer	E3
8.4.1.9 Masquerading as one network entity to an other one	A1; A2; A5; A6

Table 23: Threats with potential risk of 4 covered by the initial selection of countermeasures

Threat description	Security requirements and services
8.4.2.2 Masquerading as a network entity to delete data	A5; A6
8.4.5.4 Eavesdropping of the start of a communication on the access interface	E2
8.4.5.5 Eavesdropping of roaming number or routing number	E3
8.4.3.1 Illegal registration by an attacker masquerading as service provider	A5; A6

Assuming that the security requirements and security services are implemented as stated above, the remaining threats with major risk can be counteracted as shown in table 24.

Table 24: Remaining threats and counteracting security requirements/services

Reference and Threat description	Additional security requirements and security services	Security requirements and security services already chosen
8.4.1.8 Unauthorized access to data in terminals		C3
8.4.2.1 Eavesdropping of old address		E2
8.4.5.3 Eavesdropping of the communication on the access interface by use of the session key		C1; C2
8.4.5.6 Modification of routing data		C1; C2
8.4.6.3 Eavesdropping of the communication on the access interface by use of the session key		C1; C2; E2; E1; A1-A6
8.4.6.4 Eavesdropping of the communication on the NNI interfaces		E3
8.4.6.7 Modification of the dialled number		E2; C2
8.4.6.8 Masquerading by using someone's TIPHON-id only		A1; A2
8.4.8.2 Manipulation of transmitted information during service profile transfer	I2	
8.4.8.3 Unauthorized access to the service profile of somebody by unauthorized use of service profile interrogation		C2; C4
8.4.8.4 Unauthorized access to, or unauthorized use of, the service profile modification procedure		C2; C4

Annex A (informative): SIP specific threat analysis

A.1 Introduction

SIP is a relatively new technology (1995) developed for remote control, establishment and tear-down of multimedia sessions. The origins of SIP are in the academic and IETF community and assumed in its first incarnation a public internet although with the interest shown by 3GPP the application to a managed network that uses IP has become ascendant. SIP is based upon the communication model of HTTP and therefore is broadly viewed as a request-response protocol. In relation to other well known protocols SIP has close cousins in Remote Procedure Call (RPC) and in the ITU-T ROSE protocol.

Like HTTP SIP does not describe content in its protocol. In practice it only asks the receiver to join a communication described in an attached description. This is somewhat similar to the practice of HTTP being content unaware and the actions to be taken by the receiver of an HTTP message being contained in the HTML file generally attached (e.g. render the attached file in the browser application).

The binding of transport to the session is not explicit in SIP.

A.2 Extract from RFC 3261

SIP is not a vertically integrated communications system. SIP is rather a component that can be used with other IETF protocols to build a complete multimedia architecture. Typically, these architectures will include protocols such as the Real-time Transport Protocol (RTP) (IETF RFC 1889 [14]) for transporting real-time data and providing QoS feedback, the Real-Time Streaming Protocol (RTSP) (IETF RFC 2326 [15]) for controlling delivery of streaming media, the Media Gateway Control Protocol (MEGACO) (IETF RFC 3015 [16]) for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP) (IETF RFC 2327 [17]) for describing multimedia sessions. Therefore, SIP should be used in conjunction with other protocols in order to provide complete services to the users. However, the basic functionality and operation of SIP does not depend on any of these protocols.

SIP does not provide services. Rather, SIP provides primitives that can be used to implement different services. For example, SIP can locate a user and deliver an opaque object to his current location. If this primitive is used to deliver a session description written in SDP, for instance, the endpoints can agree on the parameters of a session. If the same primitive is used to deliver a photo of the caller as well as the session description, a "caller ID" service can be easily implemented. As this example shows, a single primitive is typically used to provide several different services.

SIP does not offer conference control services such as floor control or voting and does not prescribe how a conference is to be managed. SIP can be used to initiate a session that uses some other conference control protocol. Since SIP messages and the sessions they establish can pass through entirely different networks, SIP cannot, and does not, provide any kind of network resource reservation capabilities.

The nature of the services provided make security particularly important. To that end, SIP provides a suite of security services, which include denial-of-service prevention, authentication (both user to user and proxy to user), integrity protection, and encryption and privacy services.

SIP works with both IPv4 and IPv6.

A.3 SIP protocol, methods and responses

A.3.1 Protocol

The SIP protocol machine is very simple: Request is sent and the requestor waits for a response. The request contains the method and who the method is aimed at, the response contains the status code that informs the requestor of how the server has dealt with the request. The current version of SIP does not provide absolutely complete normal and exceptional behaviour for each method invocation. In this respect it is possible to generate behaviours that may break equipment. Furthermore as the request-response behaviour of SIP is not related to the session that any method refers to the SIP description cannot be made complete. This is a failing of any transport protocol used to report application behaviour (a similar problem may exist in RPC and ROSE), and has roots in the HTTP/HTML source of SIP.

EXAMPLE: If the session description cannot be implemented or if implemented invokes rogue behaviour in the receiver the response given by SIP has to be derived from the session description in addition to the content of the SIP message headers. If we use HTTP/HTML as analogous to SIP/SDP then a failure in a JavaScript element within the HTML may be successfully reported by HTTP as a message success as all that HTTP can measure is the ability to deliver the HTML not how it is rendered. The rendering machine identifies the error in the HTML.

A.3.2 Methods

There are 6 core methods in SIP and these are the basis of the protocol:

- INVITE - starts a session (and modifies it if used as a re-invite)
- ACK - confirms the invite
- BYE - terminates sessions
- CANCEL - stops an invite
- OPTIONS - Querying capability
- REGISTER - binds address (SIP name) to network address

A.3.2.1 Security concerns of SIP methods

There have been security problems reported with all of these methods, some severe, some not.

EXAMPLE 1: It is widely reported that the REGISTER method does not work across NAT as the network address offered initially is not valid. In order to make it work NAT has to give way to an application level gateway able to identify the REGISTER method with an address valid for the far side of the NAT.

EXAMPLE 2: The OPTIONS method can be used to trawl data from a SIP server.

EXAMPLE 3: The use of unsolicited BYE messages can give denial of service.

EXAMPLE 4: The use of unsolicited CANCEL messages can give denial of service.

A.3.3 Protocol components

The protocol of SIP is enabled by assigning particular functions to a set of protocol components. A particular SIP device will contain 1 or more of these components.

- User Agent Client (UAC)
- User Agent Server (UAS)

- Redirect server
- Proxy server
- Registrar

The UAC and UAS exist in a normal terminal device and are termed jointly the User Agent.

The proxy server arises from breaking the assumption that the UACs know the UASs that they want to communicate with. In anything but the smallest of networks this assumption is inevitably broken so a network resident proxy to the UA exists to facilitate routing.

Proxy servers can be configured to perform inter-domain call establishment.

The registrar server is a special case of a proxy server that attends to REGISTER methods. In most cases the registrar and proxy server will be co-located. In SIP the REGISTER method is not an authorization method, and in fact SIP does not offer any form of authorization protocol.

NOTE: The lack of an authorization protocol does not allow SIP to conform to the registration and service attachment service described in TS 101 882-2.

A.4 The threats and risk factors

The general threat model provided in the core document applies to a SIP phone or any other SIP entity. The threats of masquerade attack, denial of service attack, and risks associated with the confidentiality of signalling and traffic are retained. It is the ability to exploit these threats to modify the general threat analysis that is of concern.

The supposition taken is that all attacks in SIP are straightforward to implement, and moreover may be implemented by techniques not considered viable in PSTN/ISDN, which raises the likelihood of the threat occurring to "likely" which in turn modifies the risk factor (i.e. the product of likelihood and impact).

The weaknesses of SIP come in large part from the original design basis of SIP. SIP is built on the structure of HTTP whose primary purpose is to allow open access to data on a remote server. In allowing and assuming open access there needs to be no provision for secure access to data. In addition the SIP protocol is incompletely specified by allowing undocumented behaviour to be provided in an implementation. In general for TIPHON the exact and complete behaviour is defined for any service and service capability. In this respect the use of SIP in a TIPHON environment may in practice usefully restrict the threat from SIP by restricting its scope of operation. Overall of the threats in the core of the document 14 are moved into the critical risk level.

The modified risk assessment tables from the core of the document are given below:

Table A.1: Risk assessment for general threats

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.2.1 Eavesdropping of TIPHON-id on interfaces or entities	3	2	6	Initial communication at any new TpoA/SpoA may have to receive the TIPHON-id in clear
9.5.2.2 Getting the TIPHON-id from a terminal	3	2	6	If the TIPHON-id is equivalent to a "telephone number" it may be visible from the terminal. If TIPHON-id is equivalent to the IMSI used in GSM/GPRS it should not be visible to the user (reduced occurrence likelihood).
9.5.2.3 Denial of service	3	3	9	
9.5.2.4 Unauthorized access to data	3	3	9	**RISK MODIFIED BY SIP**
9.5.2.5 Flooding the network	3	3	9	Developments in distributed denial of service attacks using legitimate transport protocols and remote invocation capabilities inherent in open processing platforms have made many attacks of this form simpler to invoke, and may be invoked transparently to the owner of the attack platform.
9.5.2.6 Stolen terminals	3	2	6	
9.5.2.7 Subscription fraud	3	2	6	Risk is greater for corporate rather than individual subscriber (many terminals versus single terminal).
9.5.2.8 Unauthorized access to data in terminals	3	3	9	**RISK MODIFIED BY SIP**
9.5.2.9 Masquerading as one network entity to an other one	3	3	9	Some technology devices (gateways) may be very straightforward to clone and to mount attacks from. In particular to manipulate call processing.

Table A.2: Risk assessment for threats related to data deletion procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.3.1 Eavesdropping of old address	3	1	3	Minimize the risk by using non-global addressing. May require geographical address for location based services
9.5.3.2 Masquerading as a network entity to delete data	3	2	6	**RISK MODIFIED BY SIP**

Table A.3: Risk assessment for threats related to subscription registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.4.1 Illegal registration by an attacker masquerading as service provider	3	2	6	**RISK MODIFIED BY SIP** Service dependent.

Table A.4: Risk assessment for threats related to subscription de-registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.5.1 Illegal de-registration by an attacker masquerading as service provider	3	3	9	**MODIFIED BY SIP**
9.5.5.2 Subscriber does not allow de-registration by manipulating his terminal	3	3	9	**MODIFIED BY SIP**
9.5.5.3 Subscriber does not allow de-registration by manipulating the signalling interface	3	3	9	**MODIFIED BY SIP** For user accessible application code such as SIP manipulation may be possible by use of virus infection.

Table A.5: Risk assessment for threats related to TIPHON incoming call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.6.1 Masquerading by using someone's TIPHON-id	3	2	6	
9.5.6.2 Masquerading by using someone's TIPHON-id and authentication information	3	3	9	**RISK MODIFIED BY SIP** The design of the authentication mechanism should be sufficient to minimize the likelihood. If it is broken it will affect all on the network as the attack method may be reapplied.
9.5.6.3 Eavesdropping of the communication on the access interface by use of the session key	3	2	6	**RISK MODIFIED BY SIP** Session keys should not be exchanged in clear and have a lifetime very much less than the time required to determine the key.
9.5.6.6 Eavesdropping of the start of a communication on the access interface	3	2	6	**RISK MODIFIED BY SIP**
9.5.6.7 Eavesdropping of roaming number or routing number	3	2	6	**RISK MODIFIED BY SIP**
9.5.6.8 Modification of routing data	3	3	9	**RISK MODIFIED BY SIP** Routing data has commercial significance so will be highly protected.

Table A.6: Risk Assessment for threats related to TIPHON outgoing call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.7.1 Masquerading by using someone's TIPHON-id	3	2	6	
9.5.7.2 Masquerading by using someone's TIPHON-id and authentication information	3	3	9	**RISK MODIFIED BY SIP**
9.5.7.3 Eavesdropping of the communication on the access interface by use of the session key	3	2	6	**RISK MODIFIED BY SIP**
9.5.7.5 Eavesdropping of the communication on the NNI interfaces	3	3	9	**RISK MODIFIED BY SIP**
9.5.7.6 Eavesdropping of the start of a communication on the access interface	3	2	6	
9.5.7.7 Eavesdropping of the phone number of the called party	3	2	6	
9.5.7.8 Modification of the dialled number	3	3	9	**RISK MODIFIED BY SIP**
9.5.7.10 Masquerading by using someone's TIPHON-id only	3	1	3	**RISK MODIFIED BY SIP**

Table A.7: Risk Assessment for threats related to emergency call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.8.1 Misuse of emergency call	3	2	6	
9.5.8.2 Manipulate data to give an emergency number to somebody	3	3	9	**RISK MODIFIED BY SIP**

Table A.8: Risk assessment for threats related to service profile

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.9.1 Eavesdropping of transmitted information during Service Profile Transfer	3	3	9	**RISK MODIFIED BY SIP** Service profile is probably easier to notice than other signalling as profile is a larger construct.
9.5.9.2 Manipulation of transmitted information during Service Profile Transfer	3	3	9	**RISK MODIFIED BY SIP**
9.5.9.3 Unauthorized access to the service profile of somebody by unauthorized use of Service Profile Interrogation	3	3	9	**RISK MODIFIED BY SIP**
9.5.9.4 Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure	3	3	9	**RISK MODIFIED BY SIP**

Annex B (informative): ITU-T H.323 specific threat analysis

B.1 Introduction

The suite of standards developed by ITU-T SG16 under the H.323 umbrella are extensive and provide a means of providing application level multi-media sessions across a LAN developing into a means of providing application level multi-media sessions over a WAN, by provision of a toolbox of recommendations.

In line with the enlarging of the scope of H.323 a number of security options are provided in the H.323 suite providing public key (asymmetric), secret key (symmetric), and hybrid mechanisms to provide authenticity, integrity and confidentiality countermeasures.

B.2 Extract from H.323 (November 2000)

This recommendation covers the technical requirements for multimedia communications systems in those situations where the underlying transport is a Packet Based Network (PBN) which may not provide a guaranteed Quality of Service (QoS). These packet based networks may include Local Area Networks, Enterprise Area Networks, Metropolitan Area Networks, Intra-Networks, and Inter-Networks (including the Internet). They also include dial up connections or point-to-point connections over the GSTN or ISDN which use an underlying packet based transport such as PPP. These networks may consist of a single network segment, or they may have complex topologies which incorporate many network segments interconnected by other communications links.

This Recommendation describes the components of an H.323 system. This includes Terminals, Gateways, Gatekeepers, Multipoint Controllers, Multipoint Processors, and Multipoint Control Units. Control messages and procedures within this Recommendation define how these components communicate. Detailed descriptions of these components are contained in clause 6.

H.323 terminals provide audio and optionally video and data communications capability in point-to-point or multipoint conferences. Interworking with other H-series terminals, GSTN or ISDN voice terminals, or GSTN or ISDN data terminals is accomplished using Gateways, see figure 1. Gatekeepers provide admission control and address translation services. Multipoint Controllers, Multipoint Processors and Multipoint Control Units provide support for multipoint conferences.

The scope of H.323 does not include the network interface, the physical network, or the transport protocol used on the network. Examples of these networks include but are not limited to:

- Ethernet (IEEE 802.3);
- Fast Ethernet (IEEE 802.3u);
- FDDI;
- Token Ring (IEEE 802.5);
- ATM.

B.3 Discussion

In the core document threats are assessed for a generic communications system represented by TIPHON. As in most such systems the risks are broadly those of masquerade (of user or of network) and of loss of confidentiality. The countermeasures proposed in the core document provide the potential to reduce the risk of attack on the service platforms that TIPHON comprises of.

In H.323 there are a number of holes identified in the core specifications where security measures (countermeasures) need to be developed. The most complete of these is to be found in ITU-T Recommendation H.323 [11], annex J which offers a hybrid mechanism to provide security for Simple Endpoint Types (SET devices) themselves described in ITU-T Recommendation H.323 [11], annex F.

The structure of H.323 is not stable as annexes are added to address new capabilities, for example Quality of Service, specific endpoint types. As a consequence any security model in H.323 is likely to be deficient against the entire suite of recommendations. Furthermore the status of a recommendation in the ITU is sufficiently open to allow national or regional variants to exist which somewhat complicates the security to be achieved.

B.4 Extract from H.323 annex J

B.4.1 Secure Audio Simple Endpoint Type (SASET)

This clause describes a baseline for **secure audio simple endpoint types (SASETs)**. An example of a SASET is a secure simple phone.

B.4.1.1 Assumptions

The baseline security profile mandates the GK-routed model for secure H.323 annex F SETs. SASETs and other H.323 entities that implement this security profile (e.g. GKs) are assumed to implement the fast connect procedure.

In accordance to annex F the baseline security profile mandates the fast connect procedure with integrated key management elements but does not support H.245 tunnelling. Thus, the baseline profile does not provide means for key update and synchronization using (tunnelled) H.245 messages. SASETs implementing only the baseline security profile but still need some key-update mechanism should hang-up the call and re-connect and thereby obtain a new session key.

B.4.1.2 Overview

The baseline security is applicable in administered environments with symmetric keys/passwords assigned among the entities (SASETs-gatekeeper, gatekeeper-gatekeeper).

Table H.323-Annex J-1 summarizes all the procedures defined in H.235v2, annex D.

Table H.323-Annex J-1: Summary of Secure Audio Simple Endpoint Types (see H.235v2, annex D)

Security Services	Call Functions						
	RAS	H.225.0		H.245	RTP		
Authentication	Password HMAC-SHA1-96	Password HMAC-SHA1-96		Password HMAC-SHA1-96			
Non-Repudiation							
Integrity	Password HMAC-SHA1-96	Password HMAC-SHA1-96		Password HMAC-SHA1-96			
Confidentiality					56-bit DES	56-bit RC2-compatible	168-bit Triple-DES
Access Control							
Key Management	Subscription-based password assignment	Subscription-based password assignment	authenticated Diffie-Hellman key-exchange	Integrated H.235 session key management (key distribution, key update using 56-bit DES/ 56-bit RC2-compatible/ 168-bit Triple-DES)			

For authentication and integrity, the user shall use a password-based scheme (blue area in table H.323-AnnexJ-1). The password-based scheme is highly recommended for authentication due to its simplicity and ease of implementation. Hashing the fields in the H.225.0 messages is the recommended approach for integrity of the messages (also using the password scheme). SASETs realize authentication in conjunction with integrity using the same common security mechanism.

SASETs when deploying the voice encryption security profile (green area in table H.323-AnnexJ-1) shall implement 56-bit DES as the default encryption algorithm; SASETs may implement 168-bit Triple-DES while SASETs implementing exportable encryption may implement 56-bit RC2-compatible.

For voice confidentiality, the suggested scheme is encryption using RC2-compatible, DES or Triple-DES based on the business model and exportability requirement. Some environments that are offering already a certain degree of confidentiality may not require voice encryption. In this case, Diffie-Hellman key agreement and other key management procedures are not necessary as well.

Access control means are not explicitly described; they can be implemented locally upon the received information conveyed within H.235 signalling fields (ClearToken, CryptoToken).

This recommendation does not describe procedures for subscription-based password/secret key assignment with management and administration. Such procedures may happen by means that are not part of this annex.

SASETs may use back-end services according to the procedure described in H.235v2, appendix I.4.6.

In addition the provisions of H.235 annex F provide for strong authentication as shown in the table below.

Table F.1/H.235: Overview of the hybrid security profile

Security Services	Call Functions			
	RAS	H.225.0	H.245	RTP
Authentication	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Non-Repudiation	(possible only on first message)	(possible only on first message)		
Integrity	RSA digital signature (SHA1)	RSA digital signature (SHA1)	RSA digital signature (SHA1)	
	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	
Confidentiality				
Access Control				
Key Management	certificate allocation,	certificate allocation,		
	authenticated Diffie-Hellman key-exchange	authenticated Diffie-Hellman key-exchange		

B.4.3 Observations for TIPHON

The authentication services provided in TIPHON are based upon strong cryptographic authentication.

The confidentiality service provided in TIPHON recommends adoption of AES or equivalent modern algorithms.

The countermeasure suite available in H.323 allows adoption of most of the countermeasures defined in TS 102 165-2 [9].

B.5 The threats and risk factors

The general threat model provided in the core document applies to an H.323 phone or any other H.323 entity. The threats of masquerade attack, denial of service attack, and risks associated with the confidentiality of signalling and traffic are retained. It is the ability to exploit these threats to modify the general threat analysis that is of concern.

The supposition taken is that all attacks in H.323 are straightforward to implement, and moreover may be implemented by techniques not considered viable in PSTN/ISDN, which raises the likelihood of the threat occurring to "likely" which in turn modifies the risk factor (i.e. the product of likelihood and impact). Note though that for those elements of H.323 that use H.225.0 which is itself based upon the signalling protocol defined in Q.931 the likelihood factor may be reduced in some instances to 2 rather than 3, although if an attack is found the likelihood of subsequent attack would make this factor revert to 3.

The modified risk assessment tables from the core of the document are given below:

Table B.1: Risk assessment for general threats

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.2.1 Eavesdropping of TIPHON-id on interfaces or entities	3	2	6	Initial communication at any new TpoA/SpoA may have to receive the TIPHON-id in clear
9.5.2.2 Getting the TIPHON-id from a terminal	3	2	6	If the TIPHON-id is equivalent to a "telephone number" it may be visible from the terminal. If TIPHON-id is equivalent to the IMSI used in GSM/GPRS it should not be visible to the user (reduced occurrence likelihood).
9.5.2.3 Denial of service	3	3	9	
9.5.2.4 Unauthorized access to data	3	3	9	**RISK MODIFIED BY H.323**
9.5.2.5 Flooding the network	3	3	9	Developments in distributed denial of service attacks using legitimate transport protocols and remote invocation capabilities inherent in open processing platforms have made many attacks of this form simpler to invoke, and may be invoked transparently to the owner of the attack platform.
9.5.2.6 Stolen terminals	3	2	6	
9.5.2.7 Subscription fraud	3	2	6	Risk is greater for corporate rather than individual subscriber (many terminals versus single terminal).
9.5.2.8 Unauthorized access to data in terminals	3	3	9	**RISK MODIFIED BY H.323**
9.5.2.9 Masquerading as one network entity to an other one	3	3	9	Some technology devices (gateways) may be very straightforward to clone and to mount attacks from. In particular to manipulate call processing.

Table B.2: Risk assessment for threats related to data deletion procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.3.1 Eavesdropping of old address	3	1	3	Minimize the risk by using non-global addressing. May require geographical address for location based services
9.5.3.2 Masquerading as a network entity to delete data	3	2	6	**RISK MODIFIED BY H.323**

Table B.3: Risk assessment for threats related to subscription registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.4.1 Illegal registration by an attacker masquerading as service provider	3	2	6	**RISK MODIFIED BY H.323** Service dependent.

Table B.4: Risk assessment for threats related to subscription de-registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.5.1 Illegal de-registration by an attacker masquerading as service provider	3	3	9	**RISK MODIFIED BY H.323**
9.5.5.2 Subscriber does not allow de-registration by manipulating his terminal	3	3	9	**RISK MODIFIED BY H.323**
9.5.5.3 Subscriber does not allow de-registration by manipulating the signalling interface	3	3	9	**RISK MODIFIED BY H.323**

Table B.5: Risk assessment for threats related to TIPHON incoming call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.6.1 Masquerading by using someone's TIPHON-id	3	2	6	
9.5.6.2 Masquerading by using someone's TIPHON-id and authentication information	3	3	9	**RISK MODIFIED BY H.323** The design of the authentication mechanism should be sufficient to minimize the likelihood. If it is broken it will affect all on the network as the attack method may be reapplied.
9.5.6.3 Eavesdropping of the communication on the access interface by use of the session key	3	2	6	**RISK MODIFIED BY H.323** Session keys should not be exchanged in clear and have a lifetime very much less than the time required to determine the key.
9.5.6.6 Eavesdropping of the start of a communication on the access interface	3	2	6	**RISK MODIFIED BY H.323**
9.5.6.7 Eavesdropping of roaming number or routing number	3	2	6	**RISK MODIFIED BY H.323**
9.5.6.8 Modification of routing data	3	3	9	**RISK MODIFIED BY H.323** Routing data has commercial significance so will be highly protected.

Table B.6: Risk Assessment for threats related to TIPHON outgoing call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.7.1 Masquerading by using someone's TIPHON-id	3	2	6	
9.5.7.2 Masquerading by using someone's TIPHON-id and authentication information	3	3	9	**RISK MODIFIED BY H.323**
9.5.7.3 Eavesdropping of the communication on the access interface by use of the session key	3	2	6	**RISK MODIFIED BY H.323**
9.5.7.5 Eavesdropping of the communication on the NNI interfaces	3	3	9	**RISK MODIFIED BY H.323**
9.5.7.6 Eavesdropping of the start of a communication on the access interface	3	2	6	
9.5.7.7 Eavesdropping of the phone number of the called party	3	2	6	
9.5.7.8 Modification of the dialled number	3	3	9	**RISK MODIFIED BY H.323**
9.5.7.10 Masquerading by using someone's TIPHON-id only	3	1	3	**RISK MODIFIED BY H.323**

Table B.7: Risk Assessment for threats related to emergency call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.8.1 Misuse of emergency call	3	2	6	
9.5.8.2 Manipulate data to give an emergency number to somebody	3	3	9	**RISK MODIFIED BY H.323**

Table B.8: Risk assessment for threats related to service profile

Threat	Occurrence Likelihood	Impact	Risk	Comment
9.5.9.1 Eavesdropping of transmitted information during Service Profile Transfer	3	3	9	**RISK MODIFIED BY H.323** Service profile is probably easier to notice than other signalling as profile is a larger construct.
9.5.9.2 Manipulation of transmitted information during Service Profile Transfer	3	3	9	**RISK MODIFIED BY H.323**
9.5.9.3 Unauthorized access to the service profile of somebody by unauthorized use of Service Profile Interrogation	3	3	9	**RISK MODIFIED BY H.323**
9.5.9.4 Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure	3	3	9	**RISK MODIFIED BY H.323**

Annex C (informative): Bibliography

- http://www.wassenaar.org.
- GSM 03.20: "Digital cellular telecommunications system (Phase 2); Security related network functions".
- GSM 02.09: "European digital cellular telecommunications system (Phase 2); Security aspects".
- GSM 12.03: "Digital cellular telecommunications system (Phase 2); Security management".
- ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- ETSI TS 101 882-1: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 1: Meta-protocol design rules, development method, and mapping guideline".
- ETSI TS 101 882-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Part 2: Registration and Service Attachment service meta-protocol definition".
- ITU-T Recommendation H.225.0 Version 2: "Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems".
- ITU-T Recommendation H.235 Version 1: "Security and Encryption for H Series (H.323 and other H.245 based) multimedia terminals".
- ITU-T Recommendation H.245 Version 3: "Control Protocol for Multimedia Communication".
- ITU-T Recommendation H.323 Version 3: "Packet Based Multimedia Communication Systems".
- ITU-T Recommendation H.323 annex F: "Simple Endpoint Types".
- ITU-T Recommendation H.323 annex J: "Security for H.323 annex F".
- ITU-T Recommendation H.235 Version 2: "Security and Encryption for H Series (H.323 and other H.245 based) multimedia terminals".
- ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture".
- ETSI TS 133 105: " Universal Mobile Telecommunications System (UMTS); 3G Security; Cryptographic Algorithm Requirements".

History

Document history		
V4.1.1	February 2003	Publication