SLOVENSKI STANDARD
SIST-TS TS 102 165-2 V4.1.1:2004

01-april-2004

Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON), 4. izdaja - Definicija okvira protokola - Varnostne metode in protokoli - 2. del: Protiukrepi

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures

Ta slovenski standard je istoveten z: **TS 102 165-2 Version 4.1.1**

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TS TS 102 165-2 V4.1.1:2004 **en**

ETSI TS 102 165-2 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 2: Counter Measures

Reference
DTS/TIPHON-08005-2R4

Keywords
IP, protocol, security, VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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

Foreword

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

The present document is part 2 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.

The present document defines by means of meta-protocol, algorithm boundary conditions, and guidance text the security countermeasures identified in TS 102 165-1 [1].

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] ETSI TS 102 165-1: "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis".

[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] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[5] ISO/IEC 9798-2: "Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms".

[6] ISO/IEC 9798-3: "Information technology - Security techniques - Entity authentication - Part 3: Entity authentication using a public key algorithm".

[7] ITU-T Recommendation Z.100: "Specification and description language (SDL)".

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 given in TR 101 877 [2], TS 101 878 [3] and the following apply:

CK	Cipher Key
FE	Functional Entities
FFS	For Further Study
KSG	Key Stream Generator
KSS	Key Stream Segment
MSC	Message Sequence Chart
PDU	Protocol Data Unit
RSO	Random Seed
SDU	Service Data Unit
SpoA	Service point of Attachement
TpoA	Transport point of Attachement
TVP	Time Variant Parameter

4 Provision of counter-measures in TIPHON

4.1 Required security services

In TS 102 165-1 [1] the threats to a TIPHON system have been analysed and a set of recommended countermeasures identified that when implemented will reduce the overall risk to users of TIPHON systems. A subset of these countermeasures has been identified as essential to counter most threats.

The following security services are identified in [1] as required to minimize the risk to TIPHON to an acceptable level and are required to be standardized.

- 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.

The implementation method of these countermeasures can reduce the risk. However each countermeasure introduces new threats to the system by adding complexity, and different implementations of the same conceptual countermeasure may introduce different levels of risk. In some instances a specific countermeasure cannot be applied to a particular technology.

4.2 Location of standardization of security services

Not all security services are standardized in the present document. Table 1 identifies the location of standardized countermeasures.

Table 1: Where counter-measures are provided in TIPHON specifications

Security service	Form of standardization	Location
A1	Meta-protocol and algorithm specification	The present document, clause 6
A2	Meta-protocol and algorithm specification	The present document, clause 7
A3	Meta-protocol and algorithm specification	The present document, clause 8
A4	Meta-protocol and algorithm specification	The present document, clause 9
A5	Meta-protocol and algorithm specification	The present document, clause 10
A6	Meta-protocol and algorithm specification	The present document, clause 11
C1	Meta-protocol specification	TS 101 882-2
C2-C4	FFS	TBD
E1	Algorithm specification and application guideline	The present document, clause 12
E2	Algorithm specification and application guideline	The present document, clause 12
E3	Algorithm specification and application guideline	The present document, clause 12
E6	Application guideline	The present document, clause 12
E7	Algorithm specification and application guideline	The present document, clause 12
P1, P2, P3, P9, P10	Management framework requirements	TS 101 303

Services A1 and A5 are functionally identical and are described only once. In both cases the entity being authenticated has direct access to the shared secret, whereas the entity performing the authentication (the registrar) maintains the key to identity relationship through a third party (the authentication centre). The specific algorithms invoked in A1 and A5 may be different.

Services A2 and A6 are functionally identical and are described only once. The specific algorithms invoked in A2 and A6 may be different.

Services A3 and A4 are described in the present document as a single mutual authentication service A34.

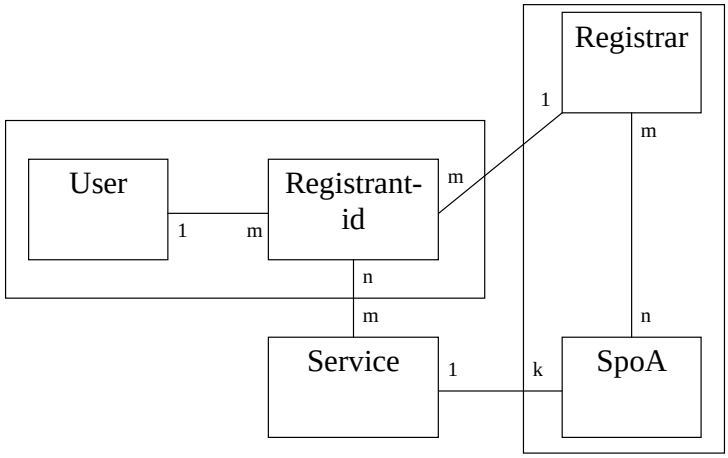
5 Authentication counter-measures

5.1 Introduction

5.1.1 Description

The primary purpose of the authentication service is to counter masquerade attacks. This may prevent attack on the system by determining that the user is legitimate, and may prevent an attack on the user by determining that the system is legitimate. The authentication services when successfully performed provide the first step in provision of access control to services (C1).

The authentication services are specified with respect to the entities and identities shown in figure 1.



NOTE 1: A single user may be associated with many registrant-ids
NOTE 2: A registrant-id shall be associated with only one user
NOTE 3: A registrant-id shall be associated with only one registrar
NOTE 4: A registrar may be associated with many registrant-ids
NOTE 5: A service may be associated with many SpoAs
NOTE 6: In any registration instance a service shall be associated with only one SpoA
NOTE 7: An SpoA shall be associated with only one Service
NOTE 8: A registrant-id may be associated with many Services

Figure 1: Ordinal relations in TIPHON

5.2 Keying policy in TIPHON

5.2.1 Release 4

In TIPHON Release 4 the policy towards keying will assume only symmetric keying methods. This method requires pre-arrangement between the authenticating entities but ensures that the authentication framework is able to provide a mapping to existing terminals which employ strong authentication (e.g. GSM, 3GPP-UMTS, DECT, TETRA).

In order to consider the authentication of the principal participants of TIPHON the following constraints on keying arise from the relations shown in figure 1.

- Registrant to Registrar shall use symmetric key authentication methods.
- Registrar to SpoA shall employ symmetric key authentication methods.
- Registrant to SpoA shall employ a symmetric session key to achieve authentication.

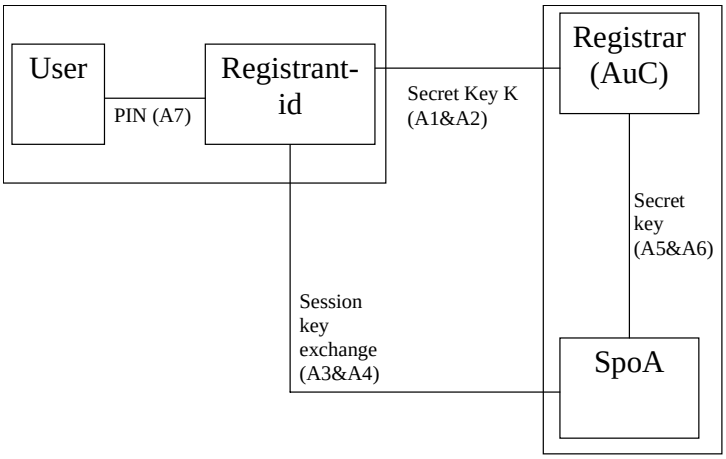


Figure 2: Key relationships in TIPHON

As a user may have many registrant-ids the user should be able to identify which to use and access to the registrant-id should be authenticated using a Personal Identification Number (PIN) or similar. The authentication service (A7) that provides for this protection of this identity is not described in this edition of the present document.

The symmetric keying authentication methods will be based upon the provisions described in ISO/IEC 9798-2 [5].

5.2.1.1 Review of service attributes

The authentication protocol should have the following properties:

- Bi-directional challenge-response type;
- Able to be initiated either explicitly or as part of the registration procedure;
- Able to be initiated by the terminal or the network;
- The recipient of the first authentication demand may instigate mutual authentication by use of a mutual authentication indicator, and by sending its challenge together with the response to the first challenge; and
- Where authentication is initiated as part of the registration the authentication timer TA shall always be less than or equal in value to any registration timer.

5.2.2 Release 5 and future

In TIPHON Release 5 and onwards the policy towards keying will encompass both symmetric and asymmetric keying methods.

The introduction of asymmetric methods may better counter the threats imposed by soft terminals and replace methods currently available that are based upon weak authentication methods (e.g. user-name and password). The public keying authentication methods will be based upon the provisions described in ISO/IEC 9798-3 [6].

6 A1 = Authentication of the terminal

6.1 Purpose

Service A1 offers strong authentication of a terminal to minimize the risk of masquerade of a terminal to the network.

6.2 Definition

The terminal shall contain a unique identity known to 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.

6.3 Description

NOTE: The mechanism here is similar to the three pass authentication method defined in ISO/IEC 9798-2 [5].

The authentication method described is a symmetric secret key type using a challenge-response protocol. In this method one secret, the authentication key (K-A1), is shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication is achieved by the parties proving to each other knowledge of the shared secret. The authenticating parties are the authentication centre attached to the registrar and the terminal representing the user.

The following sequence of events illustrates the requirement:

1) The authentication centre shall generate a random *challenge* and send it to the terminal.

2) Both parties shall generate the intermediate result *Intermediate-Result* from algorithm A1-1 using the random *challenge* and K-A1 as inputs.

3) The terminal shall generate a random *seed* for the second stage of the authentication exchange.

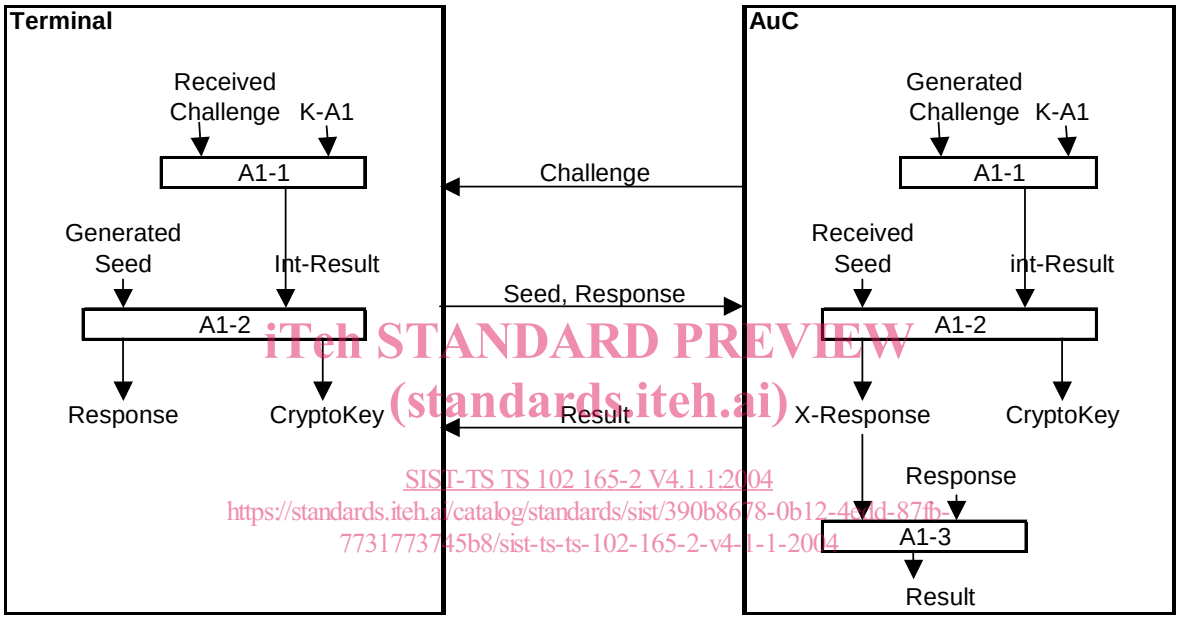
4) The terminal shall generate the cryptographic response *response* using algorithm A1-2 with inputs *seed* and *Intermediate-Result*.

5) The terminal shall send the random *seed* and the *response* to the authentication centre.

6) Upon receipt the authentication centre shall generate the expected cryptographic response using the received random *seed* and the pre-determined *Intermediate-Result* with algorithm A1-2. In addition A1-2 should generate an encryption key derived in this exchange for use in later confidentiality services.

7) The authentication centre shall compare the expected cryptographic response and the received *response*, if they are the same the terminal has proven knowledge of K-A1.

In addition to the above event sequence the protocol should be able to confirm randomness of the *challenge* and of the second stage *seed*.



NOTE: The split of the authentication algorithms allows K-A1 and algorithm A1-1 to be stored and maintained separately (remotely) from the location of A1-2.

Figure 3: Authentication service A1, algorithm invocations

6.4 Procedures

6.4.1 Provision/withdrawal

Authentication shall always be available.

6.4.2 Normal procedures

Authentication shall always be activated.

6.4.2.1 Invocation and operation

Authentication may be invoked on one or more of the following events:

- on registration to TIPHON;
- on change of physical point of attachment;
- on change of logical point of attachment;
- on demand by the user through some terminal function; and
- on demand by the authentication centre.

The registration and service attachment service defined in TS 101 882-2may be used as the master service for invocation of A1.

6.4.3 Exceptional procedures

6.4.3.1 Activation/deactivation/registration/interrogation

Not applicable.

6.4.3.2 Invocation and operation

If the expected response is not equal to the received response authentication is not proven and services A3, A4, A5 and A6 shall not be invoked. A network may reattempt service A1, however repeated failure may be considered as an attack on the algorithms and should be deterred by denying access to the initiator of the authentication.

6.5 Interactions with other TIPHON services

The authentication services are linked to the registration service and shall be operated in parallel to them.

The authentication services shall provide keying material for the confidentiality services E1, E2 and E7.

The authentication services shall provide the basis for the access control service C1.

6.6 Interworking considerations

The authentication algorithms used by each of the participant entities have to be matched.