TS 101 312 V1.3.2 (1998-06)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Scenario 1

Reference

DTS/TIPHON-02001 (c5c00j1f.PDF)

Keywords

architecture, configuration, internet, network,
protocol, telephony

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

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 ETR 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETR 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

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

1 Scope

The present document defines the network architecture, system architecture, and the reference configurations which are necessary for the delivery of telephone calls which originate in an IP network and are delivered to Switched Circuit Networks (SCN), such as Public Switched Telephone Network (PSTN), Integrated Services Digital Networks (ISDN) and Global System for Mobile communication (GSM) networks.

The present document is applicable to equipment performing the roles of terminal, gatekeeper and Gateway. Where the text indicates the status of a requirement (i.e. as strict command or prohibition, as authorization leaving freedom, or as a capability or possibility), this may modify the nature of a requirement within a referenced standard used to provide the capability.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, subsequent revisions do apply.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ITU-T Recommandation E.164 (1997): "The international public telecommunications numbering plan".

[2] ITU-T Recommandation H.323 (1998) (version 2): "Packet based multimedia communication".

[3] ITU-T Recommandation H.245 (1998) (version 3): "Control protocol for multimedia communication".

[4] ITU-T Recommandation H.225.0 (1998) (version 2): "Call signalling protocols and media stream packetization for packet based multimedia communications systems".

[5] ITU-T Recommandation H.235 (1998) (version 1): "Security and encryption for H. series [H.323 and other H.245-based] multimedia terminals".

[6] TR 101 306: "Telecommunications and Internet Protocol Harmonization Over Network (TIPHON); Requirements for service interoperability; Scenario 1".

[7] TS 101 324: "Telecommunications and Internet Protocol Harmonization Over Network (TIPHON); Naming and Addressing; Scenario 1".

3 Definitions and abbreviations

3.1 Definitions

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

gatekeeper : An H.323 entity on the IP network which provides address translation and controls access to the network for terminals, gateways, and MCUs. The gatekeeper may also provide other services to terminals, gateways and MCUs, such as bandwidth management and gateway location.

gateway: A gateway is an endpoint on a network which provides for real-time, two-way communication between terminals on an IP based network and other terminals on switched circuit network.

telephone call: Two-way speech communication between two users by means of terminals connected via network infrastructure.

terminal: An H.323 terminal (see [2]), other than a gateway or a multipoint control unit.

trust (relationship): A trust relationship is deemed to exist between two parties when those parties have mutually agreed upon some mechanism by which they can reliably establish each other's identity and that each is the source of information they exchange.

3.2 Abbreviations

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

BRAN	Broadband Radio Access Network
DECT	Digital Enhanced Cordless Telephone
GSM	Global System for Mobile communications
GW	Gateway
GK	Gatekeeper
IWF	InterWorking Function
CLI	Calling Line Identification
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Locale Access Network
MCU	Multipoint Control Unit
NNI	Network to Network Interface
OA&M	Operations, Administrations and Managament
PINX	Private Integrated services Network eXchange
PISN	Private Integrated Services Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission and Status
SCN	Switched Circuit Networks
SET	Secure Electronic Transaction
TLS	Transport Layer Security
UNI	User to Network Interface
xDSL	x Digital Subscriber Line

4 Reference configuration

This clause gives reference configurations that shall apply to telephone calls initiated in an IP network and which have a Switched Circuit Networks (SCN) as the destination network.

4.1 Reference configuration overview

The reference configuration shall consist of following entities:

- terminal connected to the IP network;
- IP access (e.g. Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN), x Digital Subscriber Line (xDSL));
- IP network;
- gateway;
- gatekeeper;
- an SCN;
- a terminal connected to an SCN network;
- back-end services;

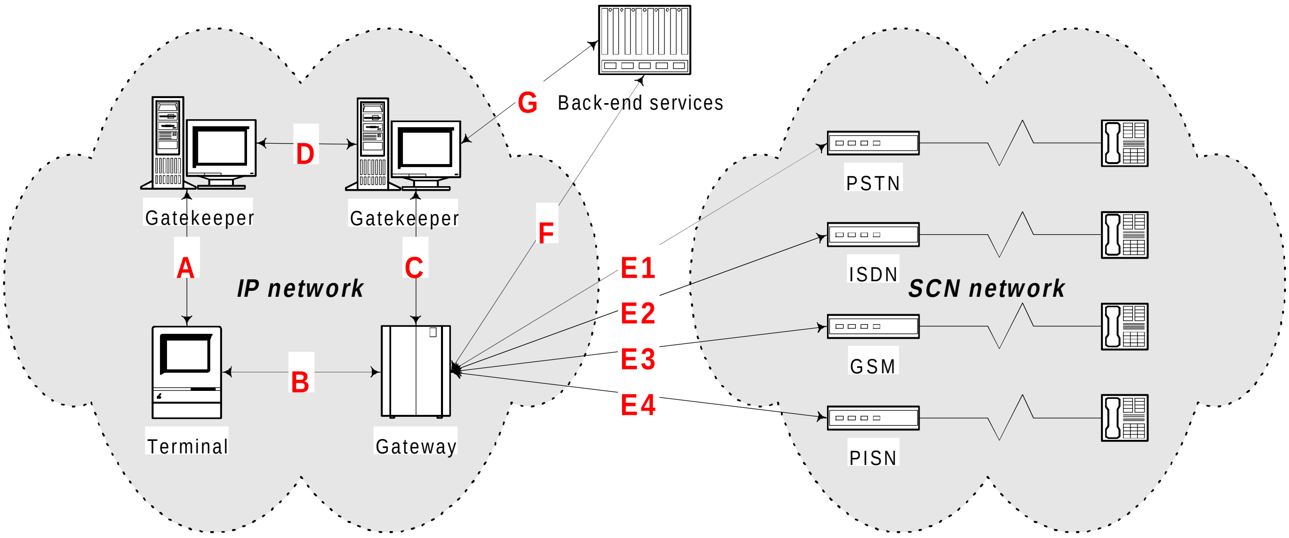

Figure 1: Basic call reference configuration

NOTE: This diagram does not represent a network topology. For example, a gatekeeper that communicates with both a terminal and a gateway is using reference points A and C.

Telephone calls originated in the IP network shall be delivered in the SCN. Interoperability shall be provided by the InterWorking Function (IWF), comprised of gatekeeper functions and gateway functions.

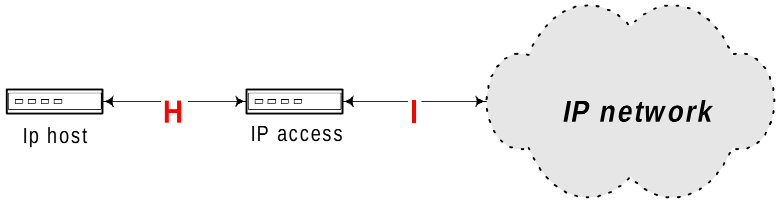

Figure 2: IP network reference configuration

4.2 Reference configuration details

The interoperability between SCN and IP networks for voice services shall have minimal impact on those networks.

The lines in the reference configuration diagram represent network connections between the elements. Dedicated or non-dedicated, long-lived or on-demand connections may be used.

4.2.1 Terminal

A terminal shall be a leaf node in the TIPHON reference configuration. It shall be a terminal connected to an IP network via some form of IP access. A terminal shall enable a user to make telephone calls to a user in the SCN. Such calls shall be under the supervision of the gatekeeper with which the user or terminal is registered.

4.2.2 IP Access

IP Access shall provide terminals, gateways, and gatekeepers access to the IP network through existing infrastructure, as shown in figure 2.

NOTE: Some examples of IP access within the TIPHON reference configuration are as follows:

- PSTN access;
- ISDN access;
- GSM access;
- xDSL access
- Cable access;
- LAN access;
- BRAN access;
- DECT access.

NOTE: This list of IP access configurations is not exhaustive; other types may be the subject of TIPHON study and specification as well. The characteristics of each IP access used may have implications for Quality of Service (QoS) and security of TIPHON calls.

4.2.3 Gatekeeper

The gatekeeper is the element in the network that shall be responsible for the Registration, Admission, and Status (RAS) of terminals and gateways.

4.2.4 Gateway

A gateway shall be physically connected to one or more IP networks and to one or more SCN networks.

4.2.5 Back-end services

Back End Services may be used by gateways and gatekeepers to provide functions (e.g. authentication function, billing and rating/tariffing, or address resolution function). These back-end services may be provided by equipment within the SCN, within the IP Network, or elsewhere.

4.3 Reference points

Nine basic reference points shall be defined as follows:

- the A reference point is between the terminal and the gatekeeper;
- the B reference point is between the terminal and the gateway;
- the C reference point is between the gateway and the gatekeeper;
- the D reference point is between two gatekeepers;
- the E reference point is between the gateway and the SCN. There are four E reference points: E1, E2, E3, and E4. The E1 reference point is associated with a PSTN. The E2 reference point is associated with an ISDN. The E3 reference point is associated with a GSM network. The E4 reference point is associated with a PISN. The protocol supported at the E reference points may be a User to Network Interface (UNI) protocol or a Network to Network Interface (NNI) protocol;
- the F reference point is between Back End Services and a gateway;
- the G reference point is between Back End Services and a gatekeeper;
- the H reference point is between an Endpoint or gatekeeper and the IP Access Network;
- the I reference point is between the IP Access Network and the rest of the IP Network.

5 Functional blocks

Three main functional blocks are identified within the IP domain: terminals, gateways, and gatekeepers. This clause contains a high-level functional model, consisting of functions identified within the main functional blocks:

5.1 Terminal

The terminal Functional Block may contain the following functional blocks:

Terminal H.225 function - receives and emits H.225 messages (see [4]);

Terminal H.245 function - receives and emits H.245 messages (see [3]);

Media channel privacy - ensures media privacy to and from the terminal;

Signalling Privacy - ensures signalling privacy to and from the terminal;

Authentication function - establishes the identity of the user, device, or network entity (see [6]);

Non-repudiation evidence gathering - collects information to be used to prove that a certain signalling or media was transmitted or received;

Management function - interfaces to the network management system; includes (but is not limited to);

Usage recording function - determines and/or records information about relevant events and resources;

Usage reporting function - reports to an external entity the determined and/or recorded usage.

5.2 Gateway (GW)

The gateway Functional Block ensures the interworking between the IP domain and the SCN domain. It may contain the following functions:

Media channel address resolution function - provides IP transport addresses for media reception and transmission;

Stream conditioning function - transfers the media streams between the IP domain and the SCN domain, including (e.g.) transcoding and echo cancellation;

GW H.225 function - receives and emits H.225 messages (see [4]);

GW H.245 function - receives and emits H.245 messages (see [3]);

SCN signalling function - receives and emits SCN signalling;

Signalling mediation function - maps between signalling in the IP domain and signalling in the SCN domain;

authentication function - establishes the identity of the user, device, or network entity (see [6]);

GW media stream admission control function - allows or disallows media streaming;

Non-repudiation evidence gathering - collects information to be used to prove that a certain signalling or media was transmitted or received;

Media channel privacy - ensures media privacy to and from the GW;

Signalling privacy - ensures signalling privacy to and from the gateway;

Management function - interfaces to the network management system;

Usage recording function - determines and/or records information about relevant events and resources;

Usage reporting function - reports to an external entity the determined and/or recorded usage.

NOTE: These functions may be made up of several sub-functions, or may be implemented in several different ways. For example, the "SCN signalling function" may be accomplished by a gateway which interfaces directly between the IP network and the ISDN network. Connection to the PSTN network or the GSM network would then be done via the ISDN network. Another option would be to use a "signalling mediation function" which would provide a generic signalling interface, and a framework which would allow multiple SCN service-providers to "plug in". The semantics of this generic signalling interface could be defined either by the signalling semantics of H.323 (see [2]) or by either of the NNI or UNI protocols of ISDN. The H.225 protocol would map to this interface, and the interface would then map to any SCN. The interface service-provider to the SCN would be responsible for converting the signalling interface to the appropriate signalling scheme along with the actual physical layer adaptation.

5.3 Gatekeeper (GK)

The gatekeeper Function shall be responsible for control and management of the various elements of the TIPHON Phase 1 reference configuration. The gatekeeper Function shall determine the route that call signalling and media transport takes for each call. It may contain the following functional blocks.

E.164 address telephone number resolution function - resolves H.323 Alias Addresses (see [2]) into full E.164-compliant Telephone Numbers (see [1]);

H.225 address resolution function - resolves H.323 Alias Addresses (see [2]) into IP transport addresses for H.225 signalling, and/or receives and emits IP transport addresses for H.225 signalling, including carrier selection;

Media channel address translation function - receives and emits IP transport addresses for media streaming, including carrier selection;

H.245 address translation function - receives and emits IP transport addresses for H.245 signalling (see [3]), including carrier selection;

GK H.225 function - receives and emits H.225 messages (see [4]);

GK H.245 function - receives and emits H.245 messages (see [3]);

Inter GK communication function - Provides to GK the means to exchange information, proxy authentication, proxy authorization, proxy registration, policy management, and accounting;

Authorization function - Provides an authorization element for services requested by entities;

Authentication function - establishes the identity of the user, device, or network entity (see [6]);

GK media stream admission control - allows or disallows media streaming;

Non-repudiation evidence gathering - collects information to be used to prove that a certain signalling or media was transmitted or received;

Signalling privacy - ensures signalling privacy to and from the terminal;

Charging function - collection of information needed to charge the user for relevant resources;

Accounting function - collection of information needed to charge another network operator or service provider for relevant resources;

Rating or tariffing function - determines the rate/tariff for usage of relevant resource(s);

Usage recording function - determines and/or records information about relevant events and resources;

Usage reporting function - reports to an external entity the determined and/or recorded usage;

Management function - interfaces to the network management system; includes (but is not limited to).

Whilst figure 1 contains two gatekeepers (in order to show the reference point between two gatekeepers), a particular TIPHON system may contain one or more gatekeepers. However, it appears to each terminal that it communicates with a single gatekeeper, and similarly for the gateway. Different gatekeepers may be responsible for different administrative domains, or for different parts of a single administrative domain.

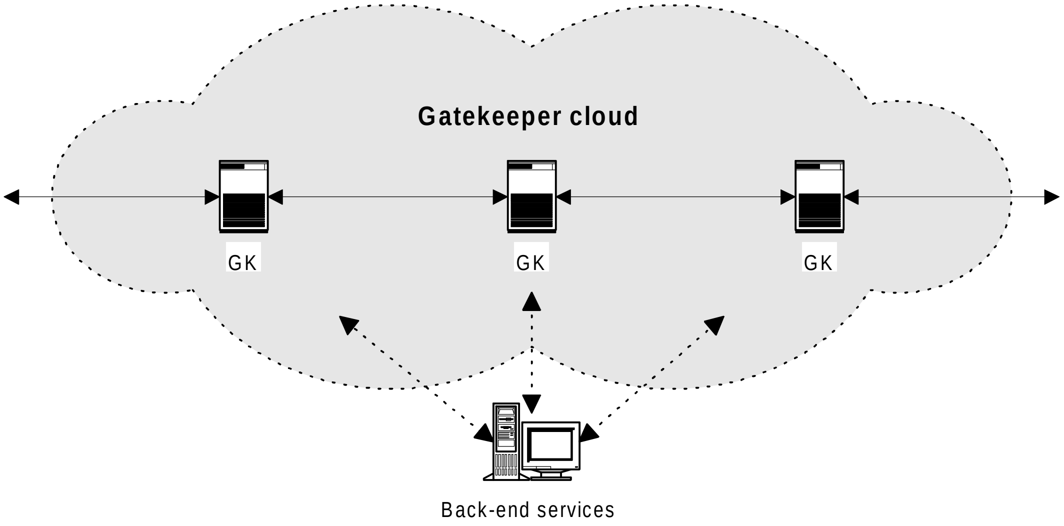

Figure 3: The GateKeeper cloud

Within the "gatekeeper cloud", the signalling may pass through one or more gatekeepers between entry to and exit from the cloud. This implies that gatekeepers may communicate information with one another when calls involve more than one gatekeeper. Dedicated or non-dedicated, long-lived or on-demand connections between GK pairs and GK-GW pairs may be used.

The gatekeeper to gatekeeper architecture is for further study.

5.4 Back-end services

Each of the functions may use various back end services.

NOTE: Examples of such services are intelligent network service control points and Remote Authentication Dial In User Service (RADIUS) authentication servers. Some of these naturally reside in the IP cloud and others in the SCN cloud. The specification of the interfaces between these Back-end services and TIPHON functions is the subject of further study.

6 Basic service scenarios

In this clause, different service scenarios are outlined. For each service scenario, a mapping on the network architecture is described.

6.1 Basic call scenarios

Two basic call scenarios shall be possible within TIPHON phase 1: A gatekeeper routed call and a direct routed call. TIPHON systems shall support gatekeeper routed calls and may support direct routed calls. In both scenarios a gatekeeper shall be required. The difference between them is that in a direct routed call, the gatekeeper shall provide the IP transport address of the terminating gateway to the calling terminal, while it does not do so in the gatekeeper routed call. The choice of which routing to use shall be determined by the calling terminal’s gatekeeper, and shall be transparent to the calling terminal.

6.1.1 Direct routed model for basic call

A gatekeeper shall be present in the TIPHON environment.

NOTE: In a direct routed basic call, Registration, Admission and Status (RAS) signalling first flows between the terminal and the gatekeeper, and then the terminal sends H.225.0 [4] and H.245 [3] signalling directly to the IP transport address of the terminating gateway.

6.1.2 Gatekeeper routed model for basic call

Signalling shall pass through a gatekeeper or a chain of gatekeepers.

NOTE: It is assumed only that each pair of gatekeepers through which the signal passes have an administrative arrangement.

7. Additional service scenarios

7.1 Calling Line Identification (CLI) and presentation numbers

TIPHON systems may convey CLI information (see [7]). This information (and an indication of how it is derived) may be provided by the network or the calling terminal. The calling party shall be able to request the restriction of the CLI presentation. The network may override this request.

Network provided numbers may be derived from information provided by devices in the IP network. This may involve the physical layer of the IP network.

7.2 Call tracing

The architecture and information flow shall enable the extraction of appropriate identification information (e.g. network number) about the calling terminal, regardless of the wishes of the calling party.

7.3 Carrier selection

TIPHON systems may convey carrier selection information, as part of the called address or otherwise (see [6] and [7]). The calling party shall be able to communicate carrier selection information to the gatekeeper and gateway.

8 Security considerations

8.1 Trust relationships

Security mechanisms for ETSI TIPHON shall support three different trust scenarios that define the relationships between administrative domains in terms of resource sharing and of external trust relationships.

NOTE: In the following scenarios, "resource" can represent both physical systems (such as terminals, gateways, and gatekeepers) and information (such as the ability to authorize a user).

8.1.1 Single administrative domain

In this scenario, shown in figure 4, all H.323 resources required for a call are contained within a single administrative domain. As there is but one domain, no external trust relationships shall be required.

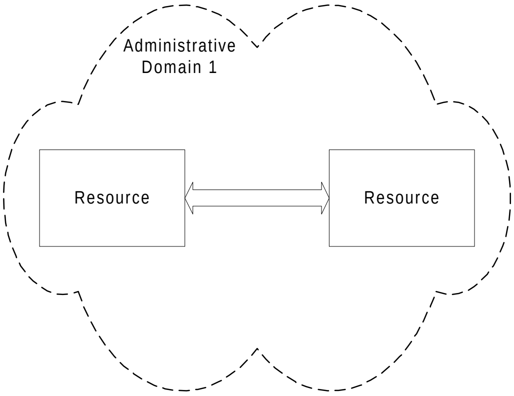

Figure 4: Single administrative domain

8.1.2 Bilateral relationship

In this scenario, shown in figure 5, the H.323 resources required for a call are divided among two administrative domains. The domains shall also have an established trust relationship. This scenario can be extended naturally to cases where more than two administrative domains are involved in a call.

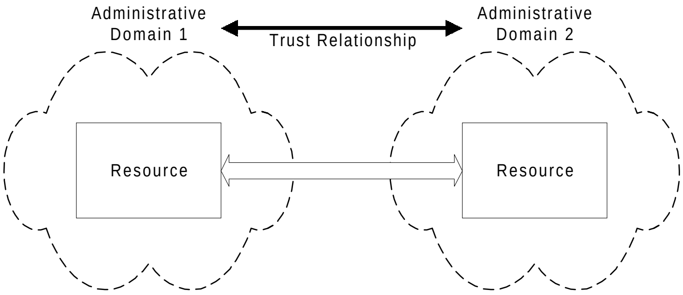

Figure 5: Bilateral relationship

8.1.3 Third party relationship

In this scenario, shown in figure 6, the H.323 resources required for a call are again divided between two administrative domains. In this case, however, the two domains do not have an established trust relationship but, each shall have a trust relationship with a third party. This scenario can be generalised to the case where more than two resources are required for the call, and to the case where the "third party" is actually multiple additional parties acting in concert. Depending on the type of resources belonging to the two administrative domains, this scenario may, in some cases, be equivalent to the bilateral relationship scenario.

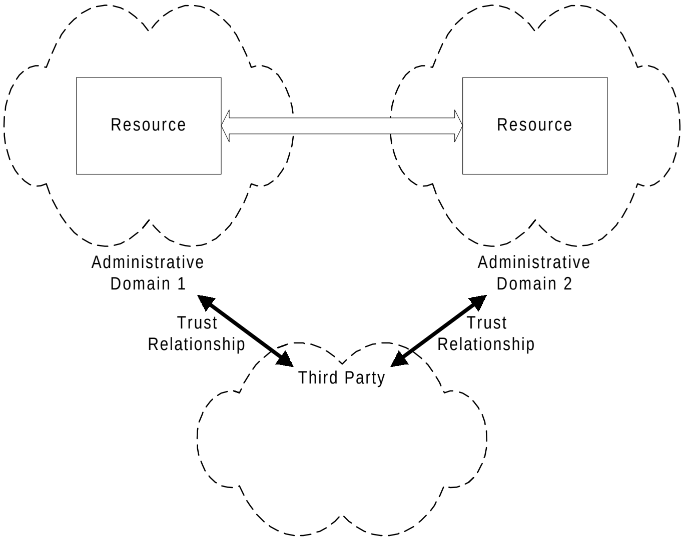

Figure 6: Third party relationship

8.2 Call phases

With an understanding of the various trust relationships that can exist for a call, that framework may be applied to the various phases of a call. This subclause describes the security architecture for several important phases in the life of a call.

8.2.1 Local (user) authentication and authorization

User authentication may be provided to allow a network element (such as a gatekeeper) and an end user to mutually establish some aspect of each other. In the case of an end user requesting service, that aspect may include the user's actual identity, or it may be simply that the user possesses coins, electronic cash, a valid Secure Exchamge Transaction (SET) account, or other financial means to pay for the call. For network elements, an end user may wish to reliably establish the element’s identity before revealing, for example, sensitive financial information. In many cases user authentication may support and lead to some form of authorization. Certain users, for example, may not be permitted to make toll calls.

NOTE: Figure 7 shows an example of this authentication phase. In it, the gatekeeper must reliably and securely establish the identity of the terminal and/or its human user. The figure’s scenario is that of a third party trust relationship because that is the most general case. Bilateral relationships and single domain environments are likely to rely on subsets of the architecture described in figure 7.

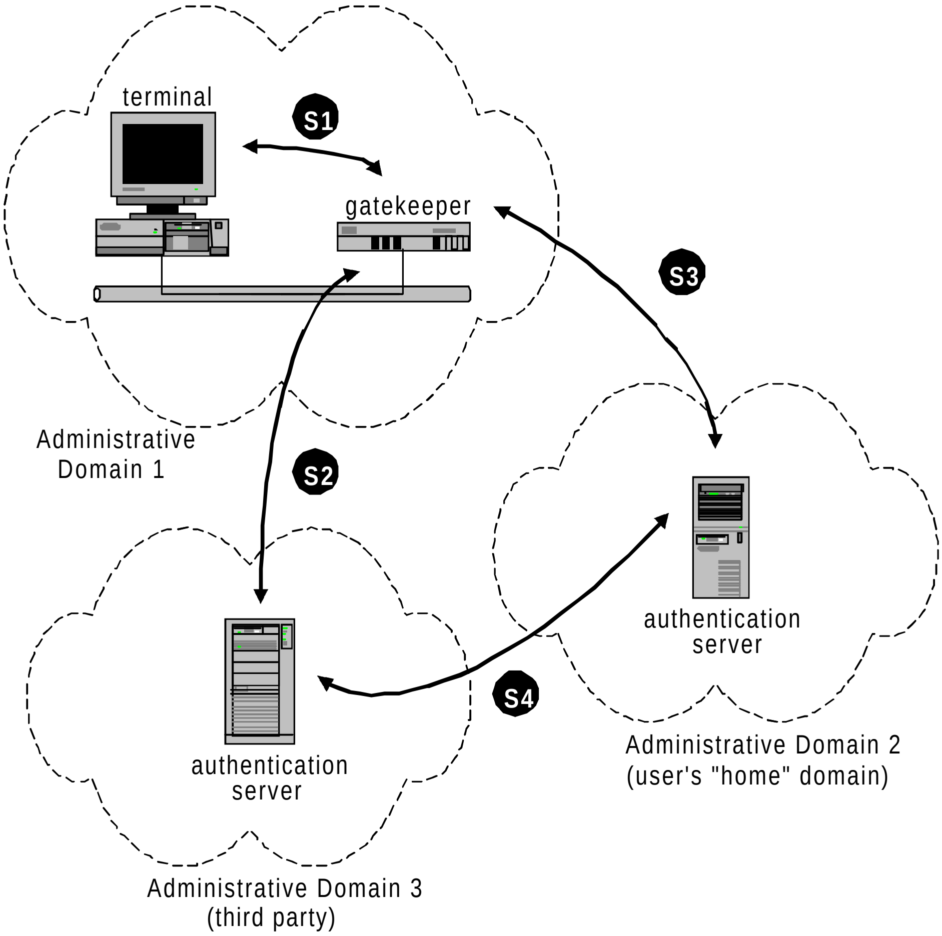

Figure 7: Security information flows - user authentication and authorization

Figure 7 identifies the following information flows:

S1: exchange of authentication and/or authorization information between terminal and gatekeeper (possibly supported by communication across the A reference point of figure 1);

S2: exchange of authentication and/or authorization information between gatekeeper and third party server (possibly supported by communication across the D or G reference points of figure 1);

S3: exchange of authentication and/or authorization information between gatekeeper and "home" domain (possibly supported by communication across the D or G reference points of figure 1);

S4: exchange of authentication and/or authorization information between third party server and user’s "home" domain (possibly supported by communication across the D or G reference points of figure 1).

NOTE 1: Figure 7 represents authentication servers as generic systems, though in some environments their roles may be served by H.323 entities such as gatekeepers.

NOTE 2: As an example, S1 may represent the RAS registration message exchange, while S2 and S4 represent user authentication via the RADIUS protocol. In such an example, no protocol need be exchanged through the S3 reference point. Note that these specific protocols are cited as examples only, and are merely intended to aid in the understanding of the architecture.

Information used to authenticate and authorize users (such as passwords) is almost certainly sensitive information and shall be protected by appropriate confidentiality measures. Such measures may include, for example, physical security of the network elements and encryption of the communication.

8.2.2 Remote (operator) authentication and authorization

Once the identity of the local user has been established, that user may be allowed to place one or more calls. With each call, the remote endpoint may authenticate and shall authorize the party attempting the call.

NOTE 1: This document distinguishes this phase from the user authentication and authorization phase because, in some trust relationships, it is a logically distinct process.

Figure 8 shows how trust relationships can influence the security architecture. It illustrates operator authentication and authorization in the context of a third party trust relationship. That relationship is the most general case. In a single domain or in bilateral relationships, some of the information flows identified in figure 8 may be unnecessary.

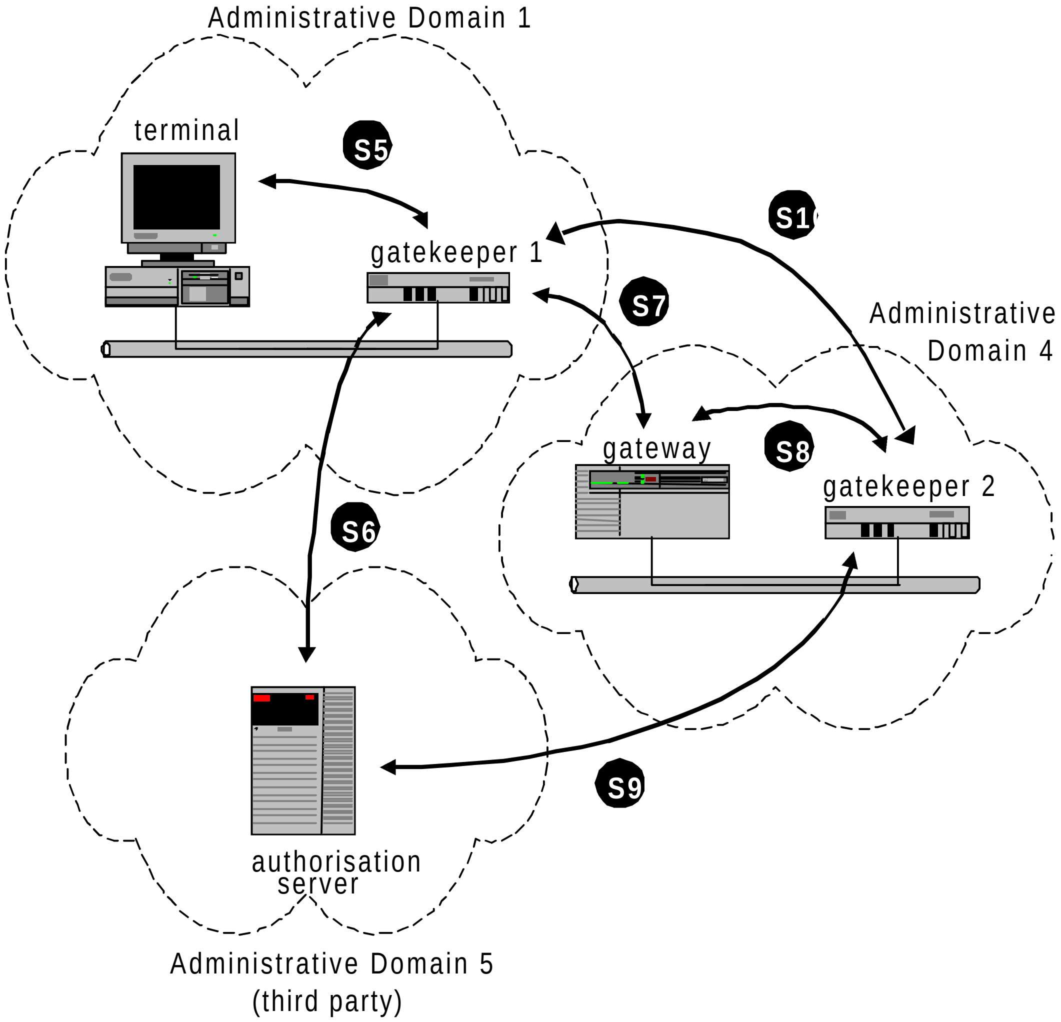

Figure 8: Security information flows for Operator authentication and authorization

Figure 8 identifies the following information flows:

S5: exchange of call authorization information between the terminal and gatekeeper 1 (possibly supported by communication across the A reference point of figure 1);

S6: exchange of call authorization information between gatekeeper 1 and third party server (possibly supported by communication across the D or G reference points of figure 1);

S7: exchange of call authorization information between gatekeeper 1 and gateway (possibly supported by communication across the C reference point of figure 1)

S8: exchange of call authorization information between gateway and its gatekeeper (possibly supported by communication across the C reference point of figure 1);

S9: exchange of call authorization information between gatekeeper 2 and third party server (possibly supported by communication across the D or G reference points of figure 1);

S10: exchange of call authorization information between gatekeepers (possibly supported by communication across the D reference points of figure 1).

NOTE 2: As a concrete example, S5 and S7 may represent H.323 Setup messages (assuming a gatekeeper-routed call), while S8 represents a RAS admission control exchange. S6 could represent a special authorization protocol, and S9 may be satisfied by the prior, out-of-band exchange of public keys. This example is not intended as an endorsement of these or any other specific protocols. Rather, it simply tries to aid in the understanding of the architecture.

NOTE 3: The figure emphasizes the fact that user authentication and authorization may differ from operator authentication and authorization. Note that neither administrative domain 2 (the user's "home" domain) nor administrative domain 3 (which authenticates the user to domain 1) appear in the figure. Of course, even though the present document makes a logical distinction between user authentication and operator authentication, it does not mean to imply that different security mechanisms are necessarily required for the two call phases. In some environments, the same mechanisms and protocols may serve both functions.

NOTE 4: As with user authentication, the information exchanged to effect operator authentication must be protected by appropriate confidentiality and privacy mechanisms.

8.2.3 Call signalling

During call setup, some environments may require that call setup information be protected from eavesdropping. Users, for example, may wish that the called number be kept confidential. figure 9 identifies information flow S11 as the point through which call signalling messages are exchanged.

NOTE 1: for clarity the figure only shows the two endpoints of the call. S11 is intended to indicate any point through which call signalling passes. For gatekeeper-routed calls, for example, S11 would also apply to the interface between endpoints and gatekeepers.

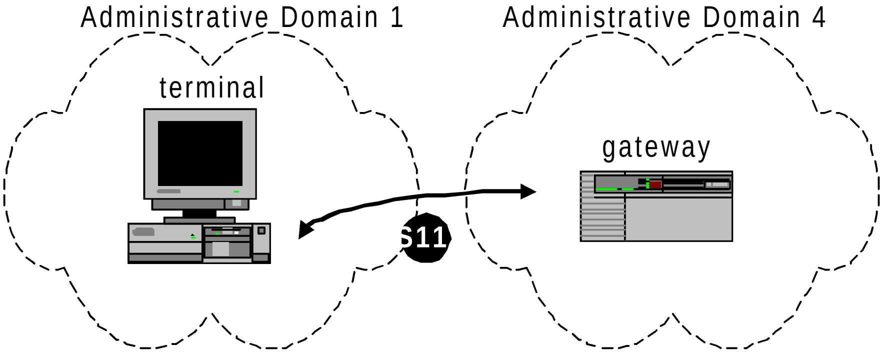

Figure 9: Security information flows for call signalling

Figure 9 identifies the following information flow:

S11: secure call signalling interface between endpoints and/or gatekeepers (possibly supported by communication across the A, B, C, or D reference points of figure 1).

NOTE 2: As an example of the use of S11, it may represent the use of the Transport Layer Security (TLS) protocol as specified in H.235 (see [5]).

8.2.4 Call Activity

Once a call is established and active, it may require security services such as media stream privacy. Figure 10 designates S12 as the information flow for media stream privacy.

NOTE 1: As with figure 9, gatekeepers are omitted for clarity.

Should any media streams be routed through a gatekeeper, S12 shall also apply.

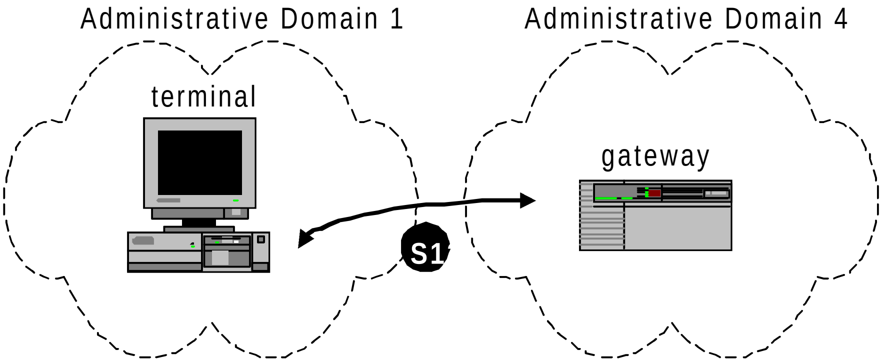

Figure 10: Security information flows for call activity

Figure 10 identifies the following information flow:

S12: secure media stream interface between endpoints and/or gatekeepers (possibly supported by communication across the A, B, C, or D reference points of figure 1).

NOTE 2: S12, for example, may represent the media stream privacy of H.235.

8.2.5 Call clearing

When a device other than the end users participating in a call (e.g. a gatekeeper) wishes to clear a call, that device shall establish its authority. A security architecture may also be important, however, in the simple case of end user call clearing. Security may be important in the third party trust relationship. In that relationship, the third party may not control either endpoint in a call, and may not know directly when the call is cleared. That third party, though, facilitated the call through its trust relationships, and as a result may have an economic stake in the call. The economic stake may require that the third party know securely and reliably when the call is cleared. Figure 11 identifies the information flows.

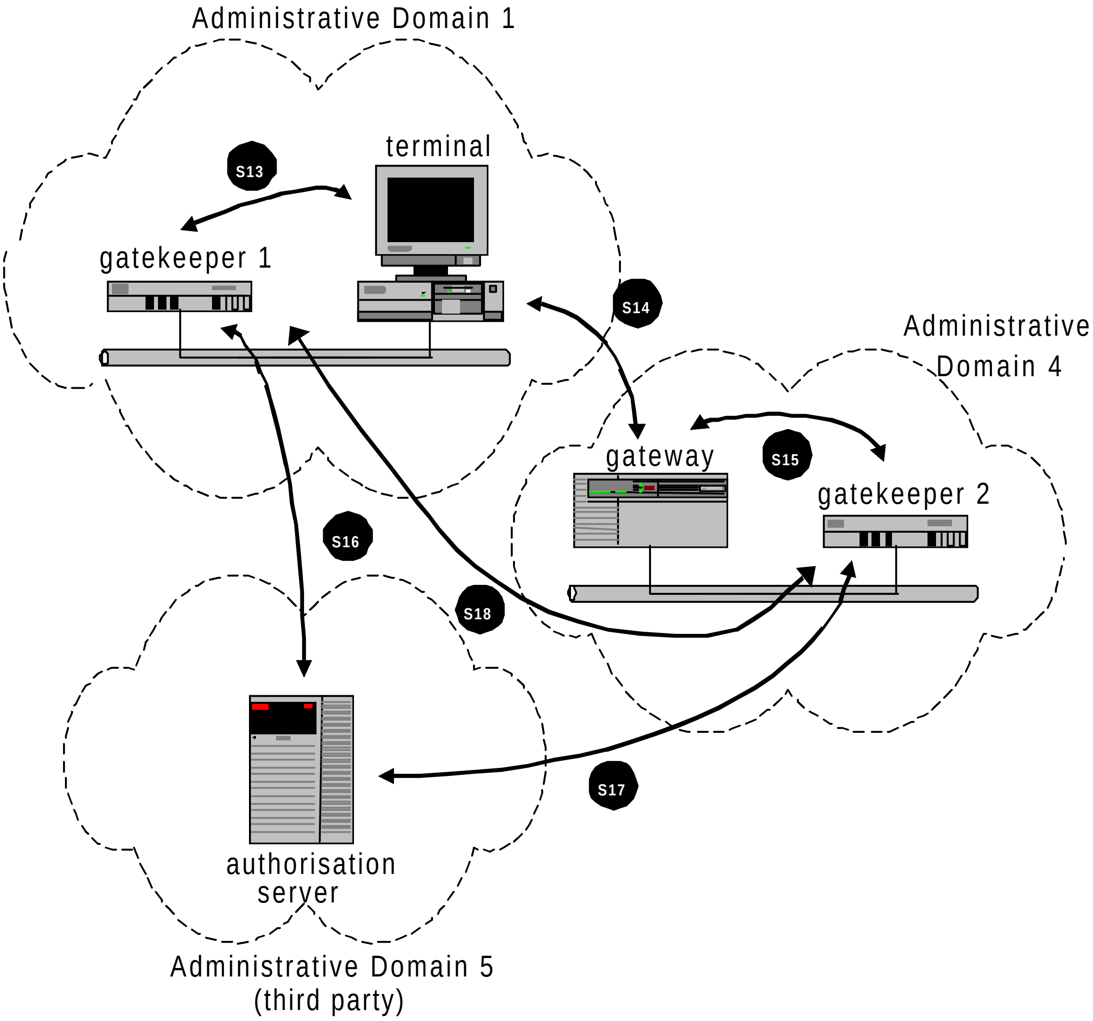

Figure 11: Security information flows for call clearing

Figure 11 identifies the following information flows:

S13: secure call clearing interface between the terminal and its gatekeeper (possibly supported by communication across the A reference point of figure 1);

S14: secure call clearing interface between endpoints (possibly supported by communication across the A, B, C, or D reference points of figure 1);

S15: secure call clearing interface between gateway and its gatekeeper (possibly supported by communication across the C reference point of figure 1);

S16: secure call clearing interface between gatekeeper 1 and third party authorizer (possibly supported by communication across the D or G reference points of figure 1);

S17: secure call clearing interface between gatekeeper 2 and third party authorizer (possibly supported by communication across the D or G reference points of figure 1);

S18: secure call clearing interface between gatekeeper 1 and gatekeeper 2 (possibly supported communication across the D reference point of figure 1).

9 Operations, Administration, and Management (OA&M)

The requirements concerning operations, administration, and management of TIPHON systems will be within scope of future issues of this specification.

History

Document history		
V1.3.2	June 1998	Publication

ISBN 2-7437-2187-1
Dépôt légal : Juin 1998