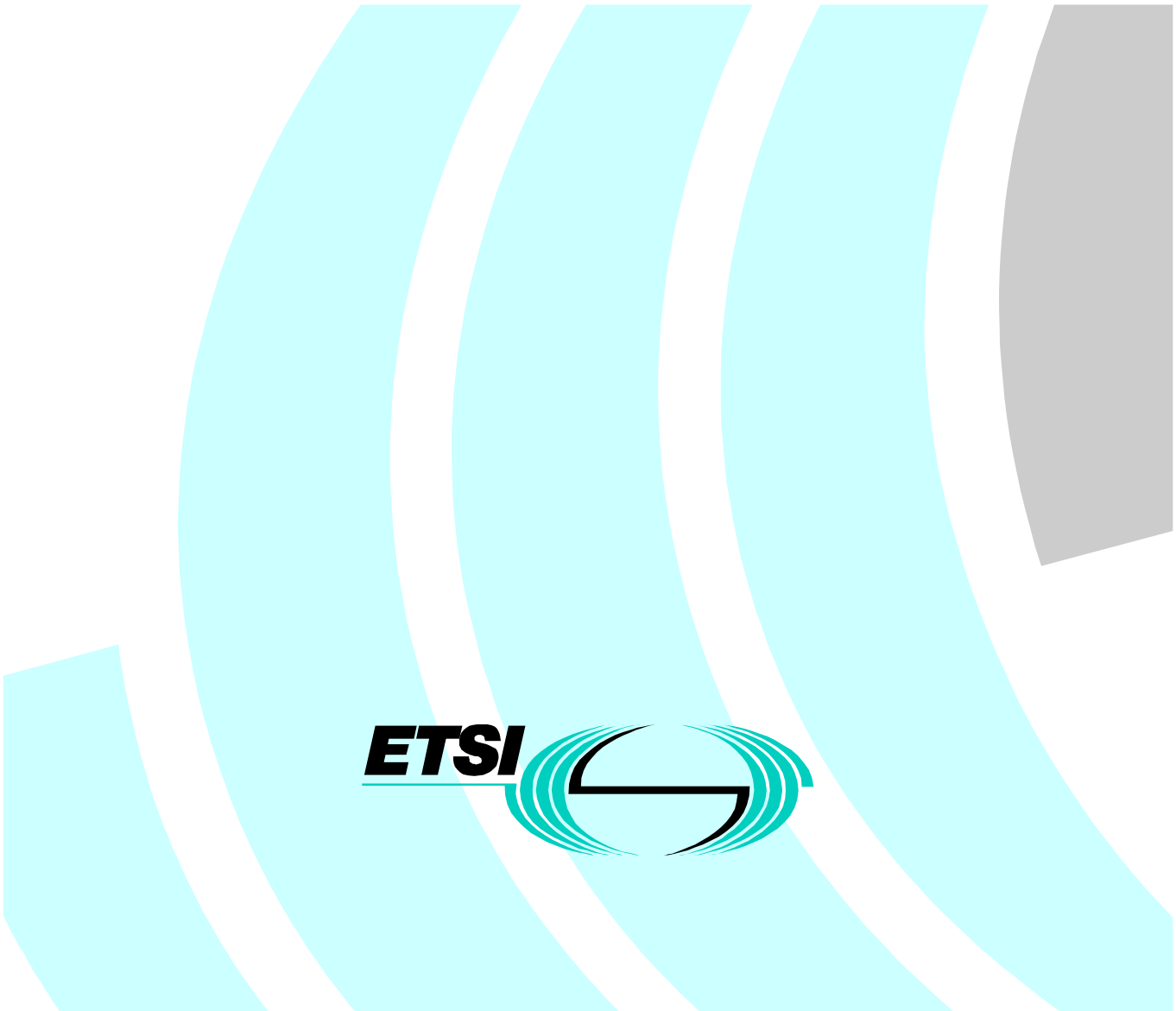
TS 101 313 V0.4.2 (1999-02)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Network architecture and reference configurations; Phase II: Scenario 1 + Scenario 2



Reference
DTS/TIPHON-02002 (c5o001df.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
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

List of Figures

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 SR 000 314: *"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.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical 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 (according to TIPHON Scenario 1).
- The delivery of telephone calls which originate in SCNs and are delivered in an IP network (according to TIPHON Scenario 2).

These two scenarios are part of TIPHON Phase 2. 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, the latest version applies.
- 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 telecommunication numbering plan".

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

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

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

[5] ITU-T Recommandation H.235 (1998): "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 Networks (TIPHON); Requirements for service interoperability; Scenario 1".

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

[8] ITU-T Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies".

[9] ITU-T Recommendation G.723.1: "Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s".

[10] ITU-T Recommendation Q.931: "ISDN user-network interface layer 3 specification for basic call control".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and 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.

Media Gateway: Provides the media mapping and/or transcoding functions.

Media Gateway Controller: Controls the Media Gateways.

Signalling Gateway: Provides the signalling mediation function between the IP domain and the SCN domain.

3.2 Abbreviations

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

ATM	Asynchronous Transfer Mode
BRAN	Broadband Radio Access Network
CLI	Calling Line Identification
DECT	Digital Enhanced Cordless Telephone
DTMF	Dual Tone Multi Frequency
GK	GateKeeper
GSM	Global System for Mobile communications
GW	Gateway
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	Integrated Services User Part
IWF	InterWorking Function
LAN	Local Access Network
MCU	Multipoint Control Unit
MG	Media Gateway
MGC	Media Gateway Controller
MTP	Message Transfer Part
OA&M	Operations, Administrations and Management
OAM&P	Operations, Administrations, Management and Provisioning
PCM	Pulse Code Modulation
PNNI	Private Network to Network Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission and Status
RTCP	Real-Time Transport Control Protocol

RTP	Real-Time Transport Protocol
SCN	Switched Circuit Networks
SCP	Service Control Point
SET	Secure Exchange Transaction
SG	Signalling Gateway
SS7	Signalling System N°7
SSP	Service Switching Point
TCAP	Transaction Capabilities Application Part
TLS	Transport Layer Security
UDP	User Datagram Protocol
UNI	User to Network Interface
xDSL	x Digital Subscriber Line

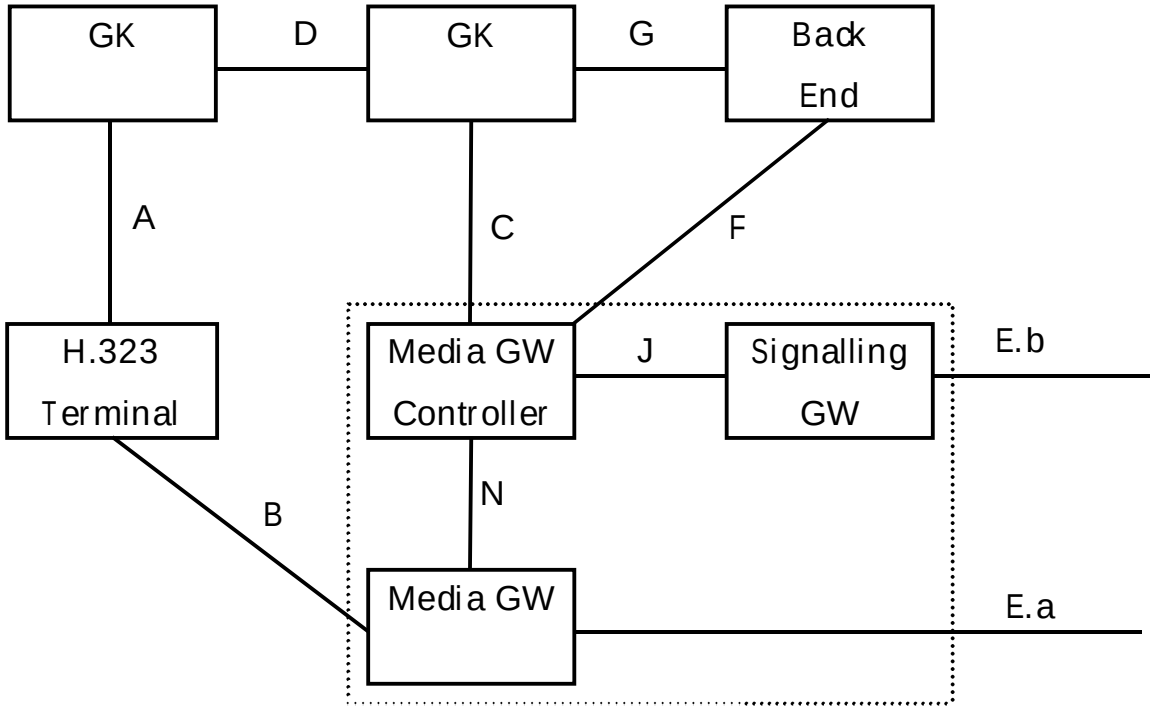
4 Reference configuration

This clause gives reference configurations that shall apply for the interworking function (IWF) to ensure service interoperability for TIPHON phase 2 systems.

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;
- Media Gateway Controller;
- Media Gateway;
- Signalling Gateway;
- gatekeeper;
- an SCN;
- a terminal connected to an SCN network;
- back-end services.



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.

Figure 1: Basic call reference configuration

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 (i.e. one administrative domain may contain multiple gatekeepers).

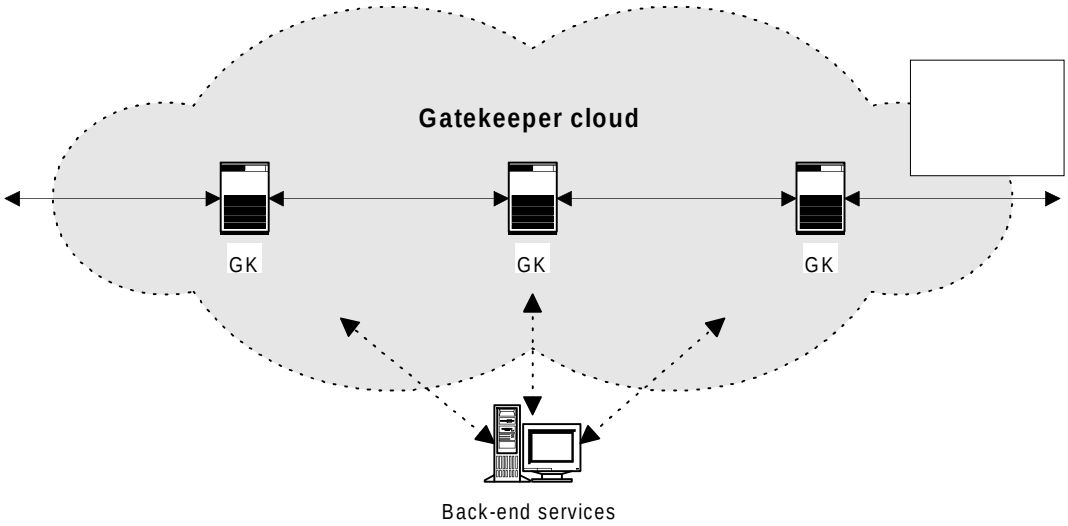


Figure 2: The GateKeeper cloud

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.

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

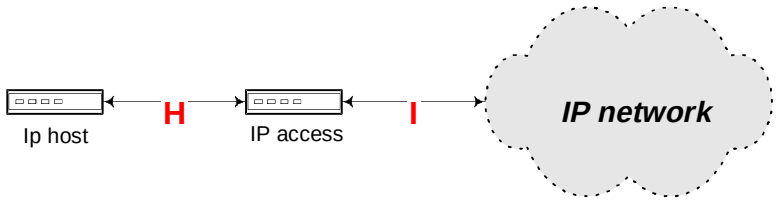


Figure 3: IP network reference configuration

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 (see 4.2.2). 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 1: 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 2: 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. The gatekeeper shall participate in zone management, call processing and call signalling.

4.2.4 Gateway

A gateway shall be physically connected to one or more IP networks and to one or more SCN networks. A gateway is composed of:

- a Signalling Gateway;
- a Media Gateway;
- a Media Gateway Controller.

One or more of these different functions can be co-located and may also be combined with gatekeepers or with other gateways.

4.2.4.1 Signalling Gateway

The Signalling Gateway provides the signalling mediation function between the IP domain and the SCN domain. It may support functional or signalling mediation between the IP domain (e.g. H.323) and call signalling in the SCN domain (e.g. channel associated signalling, non - channel associated signalling, …).

4.2.4.2 Media Gateway

The Media Gateway provides the media mapping and/or transcoding functions. It maps (e.g. tandem free operation) or transcodes the media in the IP domain (e.g. media transported over RTP/UDP/IP) and media in the SCN domain (e.g. PCM encoded voice, GSM, etc.).

4.2.4.3 Media Gateway Controller

The Media Gateway Controller sits between the Media Gateway, the Signalling Gateway and the Gatekeeper. It provides the call processing (call handling) function for the Gateway. It controls the Media Gateways; it receives SCN signalling information from the Signalling Gateway and IP signalling from the Gatekeeper.

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, etc.). These back-end services may be provided by equipment within the SCN, within the IP Network, or elsewhere.

4.3 Reference points

Ten basic reference points shall be defined as follows:

- the A reference point is between the H.323 terminal and its gatekeeper;
- the B reference point is between the H.323 terminal and the gateway (Media Gateway);
- the C reference point is between the gateway (Media Gateway Controller) and the gatekeeper;
- the D reference point is between two gatekeepers;
- the E.a reference point is between the gateway (Media Gateway) and the SCN;
- the E.b reference point is between the gateway (Signalling Gateway) and the SCN;
- the F reference point is between back-end services and a gateway (Media Gateway Controller);
- 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;

- the J reference point is between the Signalling Gateway and the Media Gateway Controller;
- the N reference point is between the Media Gateway Controller and the Media Gateway.

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.225.0 function: receives and emits H.225.0 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 is composed of three separate Functional Blocks:

- the Signalling Gateway;
- the Media Gateway;
- the Media Gateway Controller.

5.2.1 Media Gateway

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.

Codec translation function: routes the media streams between the IP domain and the SCN domain.

Media channel privacy: ensures media privacy to and from the GW.

Circuit Network Media Termination: this includes all lower-layer circuit network hardware and protocols, including the method by which speech is placed on the wire, e.g. PCM A-law, PCM Mu-law, etc.

Packet Media Termination: this includes all protocols involved in putting media over the packet network, including the codecs used. For H.323 this includes RTP/RTCP as described in H.225.0, and also the coders such as G.711, G.723.1. etc.

SCN Circuit Interface: terminates the bearer channel (e.g. DS0) from the SCN and makes it available to the Media Processing functions.

Packet/Circuit Media Processing Function: converts between audio, fax or data bearer channels on the SCN side and data packets (e.g. RTP/UDP/IP, or ATM) on the packet network side. This also performs associated signal processing functions such as voice compression, network echo-cancellation, silence suppression, comfort noise generation, encryption, fax conversion, and analogue modem conversion (for passing analogue modem signals "transparently" through the packet network). In addition, this function performs the conversion between DTMF tones on the SCN side and the appropriate signals on the packet network side when the speech codec is not transparent to DTMF. The SCN/Packet Media Processing function may also collect the packet traffic and quality data experienced by each call for use in call detail reporting and call control.

Service Circuit Function: provides services such as playing announcements and tones towards either the SCN or packet network. This function may also provide capabilities to collect and generate DTMF digits, perform voice recognition, etc. The Service Circuit function resources again are managed from within the Media Gateway and may be requested by more than one Call Control function or other external system (e.g., SCP). Some or all of these functions may be provided by an external entity in which case this function may be optional.

Usage recording function: determines and/or records signalling and/or media reception and transmission**.**

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

OAM&P: operations, administration, maintenance, and provisioning information that is not directly needed for call control can be passed through a logically separate interface to an element management system. This operations interface is beyond the scope of this paper.

Management function: interfaces to the network management system.

Packet Network Interface: terminates packet network.

5.2.2 Media Gateway Controller

GW H.225.0 function: receives and emits H.225.0 messages (see [4]).

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

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.

Packet Signalling: this includes all "call like" signalling that might exist on the packet network and is carried out by an endpoint on such a network. For H.323, this includes H.225.0, Q.931-like call signalling, H.225.0 RAS, and H.245. For an H.323 receive-only endpoint, this includesH.225.0 RAS, but not H.245.

Packet Network Signalling Interface: terminates the packet network signalling protocol (e.g., H.323, UNI, PNNI, etc.) It maintains only enough call state information to manage the protocol interface. Strictly speaking, the Packet Network Signalling Interface that exists in the Media Gateway Controller has no direct interface to the Media Gateway as all information passes from it to the Media Gateway via the Call Control Function. In general this function will reside in the Media Gateway Controller.

Gateway Control: this includes all connection control logic, resource management, and protocol translation (e.g. SS7 to H.225.0) that might take place.

Remote Resource Monitoring: maintains the Gateway Controller’s view of network-level resources available for calls. These include such things as Media Gateway trunk utilization and availability, IP network bandwidth and utilization, etc. useful for making call routing decisions.

Call Control Function: maintains the Gateway call state. The Call Control function contains all connection control logic of the Gateway. The Call Control function may interface with backend services, which may include IN services (SCP or SSP).

NOTE: This function may perform call routing, authorization, authentication, quality of service selection, billing data and per-call information recording and resource identification functions.

It communicates bearer trunk circuit termination (DS0 channel) and data network addressing, security and configuration information (voice coder, echo cancellation parameters, encryption tokens, etc.) to the Media Gateway.

Media Gateway Resource Management: allocates internal resources within the media gateway.

Signalling mediation function: maps between signalling in the IP domain (e.g. H.323) and signalling in the SCN domain, in co-operation with the Signalling Gateway.

Usage recording function: determines and/or records signalling and/or media reception and transmission.

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

OAM&P: operations, administration, maintenance, and provisioning information that is not directly needed for call control can be passed through a logically separate interface to an element management system. This operations interface is beyond the scope of this paper.

Management function: interfaces to the network management system.

Packet Network Interface: terminates packet network.

5.2.3 Signalling Gateway

Termination of lower layer protocols beneath the SCN call control protocol (e.g. MTP, etc.).

Termination of signalling from SCN: in co-operation with the signalling mediation function of the Media Gateway Controller.

Signalling mediation function: maps between signalling in the IP domain (e.g. H.323) and SCN signalling, in co-operation with the Media Gateway Controller.

Signalling privacy: ensures signalling privacy to and from the gateway.

Usage recording function: determines and/or records signalling and/or media reception and transmission.

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

OAM&P: operations, administration, maintenance, and provisioning information that is not directly needed for call control can be passed through a logically separate interface to an element management system. This operations interface is beyond the scope of this paper.

Management function: interfaces to the network management system.

Packet Network Interface: terminates packet network.

5.3 GateKeeper (GK)

The gatekeeper Function shall be responsible for control and management of the various elements of the TIPHON Phase 2 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.

SCN Address resolution function: resolves SCN Addresses into H.323 Aliasses.

H.323 Alias resolution function: resolves H.323 Alias Addresses (see [2]) into full SCN Addresses (e.g. E.164 Telephone Numbers (see [1])).

H.225.0 address resolution function: resolves H.323 Alias Addresses (see [2]) into IP transport addresses for H.225.0 signalling, and/or receives and emits IP transport addresses for H.225.0 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.225.0 function: receives and emits H.225.0 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.

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 Requirements for the reference points

6.1 Reference point A

Information flows at reference point A shall support call signalling and call information which includes H.225.0 and H.245 as described and referenced in H.323.

6.2 Reference point B

Information flows at reference point B shall support media flows between the H.323 terminal and the Media Gateway, comprising RTP and optionally RTCP as described in H.225.0 and referenced in H.323.

6.3 Reference Point C

Information flows at reference point C shall support call signalling and call information which includes H.225.0 and H.245 as described and referenced in H.323.

6.4 Reference point D

Information flows at reference point D shall support following functions:

- Discovery,

  the mechanism by which Gatekeepers discover other Gatekeepers.

- Information Exchange,

  where one Gatekeeper lets another know what (for example) dialling plans are supported, what services and devices are available, etc.

- Authentication,

  where two Gatekeepers authenticate each others identity to enable authenticated communications.

- Privacy,

  where two Gatekeepers secure their communications to insure privacy.

- Proxy Authentication,

  when a gatekeeper authenticate the identity of an entity (on behalf of that entity) with another Gatekeeper. This is usually in the Context of Proxy Registration or Authorization.

- Proxy Registration,

  where a gatekeeper registers on behalf of an entity with a remote gatekeeper.

- Proxy Authorization,

  when a gatekeeper authorize some action an entity wishes to perform (such as making a call, on behalf of that entity) with a remote gatekeeper.

- Admission Policy,

  where a Gatekeeper is asked to authorize some action on behalf or an entity or another Gatekeeper (see Proxy Authorization), and acts according to some policy profile.

- Call Signalling,

  where the actual call signalling is passed between Gatekeepers.

- Accounting,

  exchange of accounting information.

6.5 Reference point E

The information flow at the E reference point may be split in to the following.

- reference point E.a that supports media flows between the IP network and the SCN;
- reference point E.b that supports signalling between the IP network and the SCN.

6.6 Reference point F

For further study.

6.7 Reference point G

For further study.

6.8 Reference point J

For further study.

6.9 Reference point N

Information flows at reference point N shall include support for the following functions:

1) creation, modification, and deletion of media stream connections across the Media Gateway;

2) specification of the transformations to be applied to media streams as they pass through the Media Gateway, when as connections are created and subsequently during the life of the connection;

3) requesting the insertion of tones and announcements into media streams, either by explicit request of the Media Gateway Controller or by indicating that insertion should begin and end with the detection of specified events within the Media Gateway itself;

4) requesting the reporting of, and possibly specifying the actions to take upon detection of specified events within the media streams.

7 Basic service scenarios

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

7.1 Basic call scenarios

Two basic call scenarios shall be possible within TIPHON phase 2: 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.

7.1.1 Direct routed model for basic call

A gatekeeper shall be present in the TIPHON environment. Direct routed calls are outside the scope of the present document.

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.

7.1.2 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.

8 Additional service scenarios

8.1 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 IP network or the calling terminal. The calling party shall be able to request the restriction of the CLI presentation. The IP network may override this request.

IP 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.

8.2 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.

8.3 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.

9 Security considerations

9.1 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).

9.1.1 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.

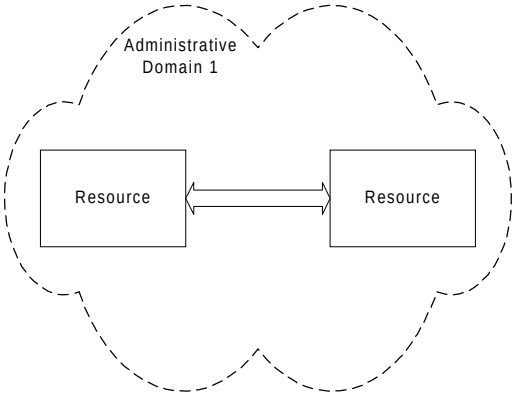


Figure 4: Single administrative domain

9.1.2 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.

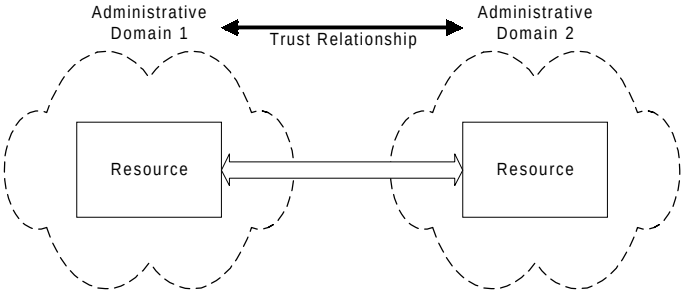


Figure 5: Bilateral relationship

9.1.3 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 generalized 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.

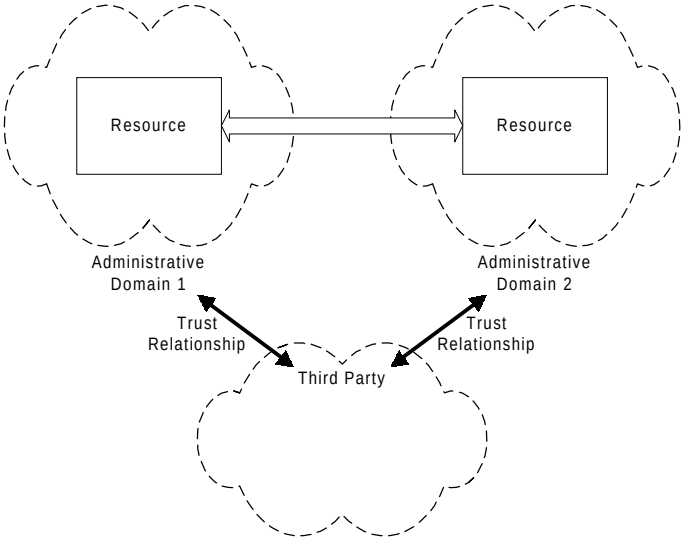


Figure 6: Third party relationship

9.2 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.

9.2.1 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 Exchange 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 1: Figure 7 shows an example of this authentication phase. In it, the gatekeeper should 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.

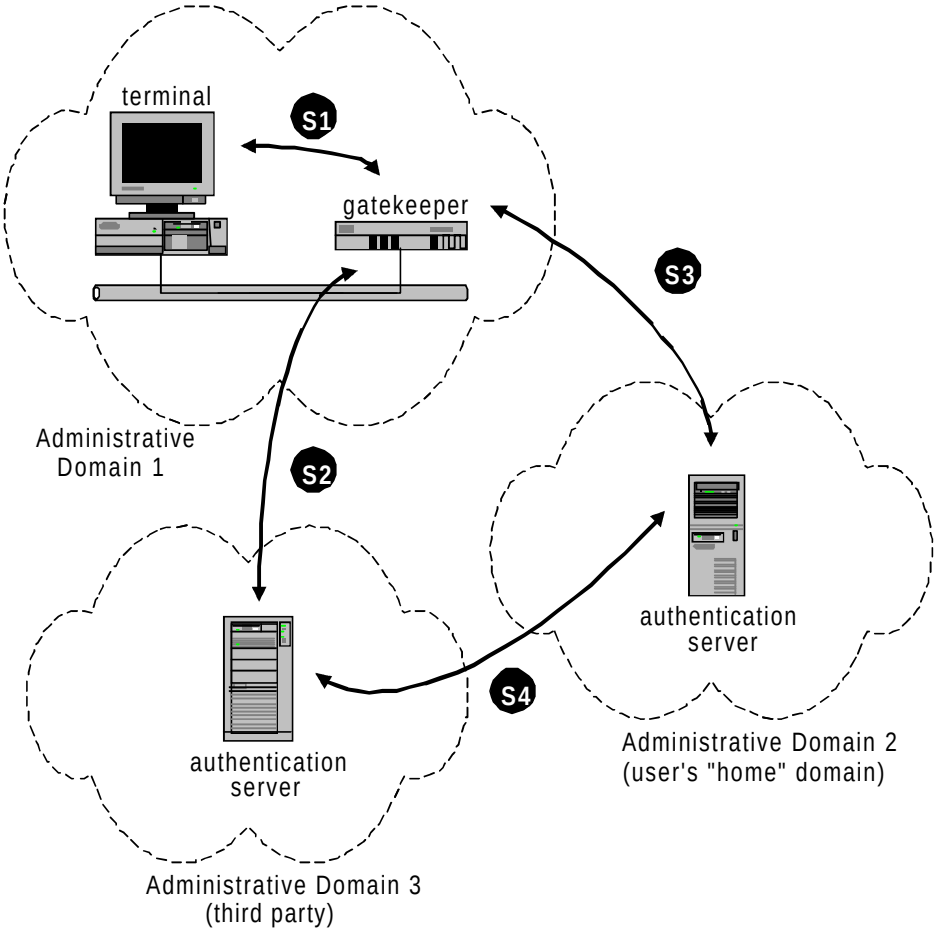


Figure 7: Security information flows - user authentication and authorization

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 2: Figure 8 represents authentication servers as generic systems, though in some environments their roles may be served by H.323 entities such as gatekeepers.

NOTE 3: 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.

9.2.2 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: The present 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.

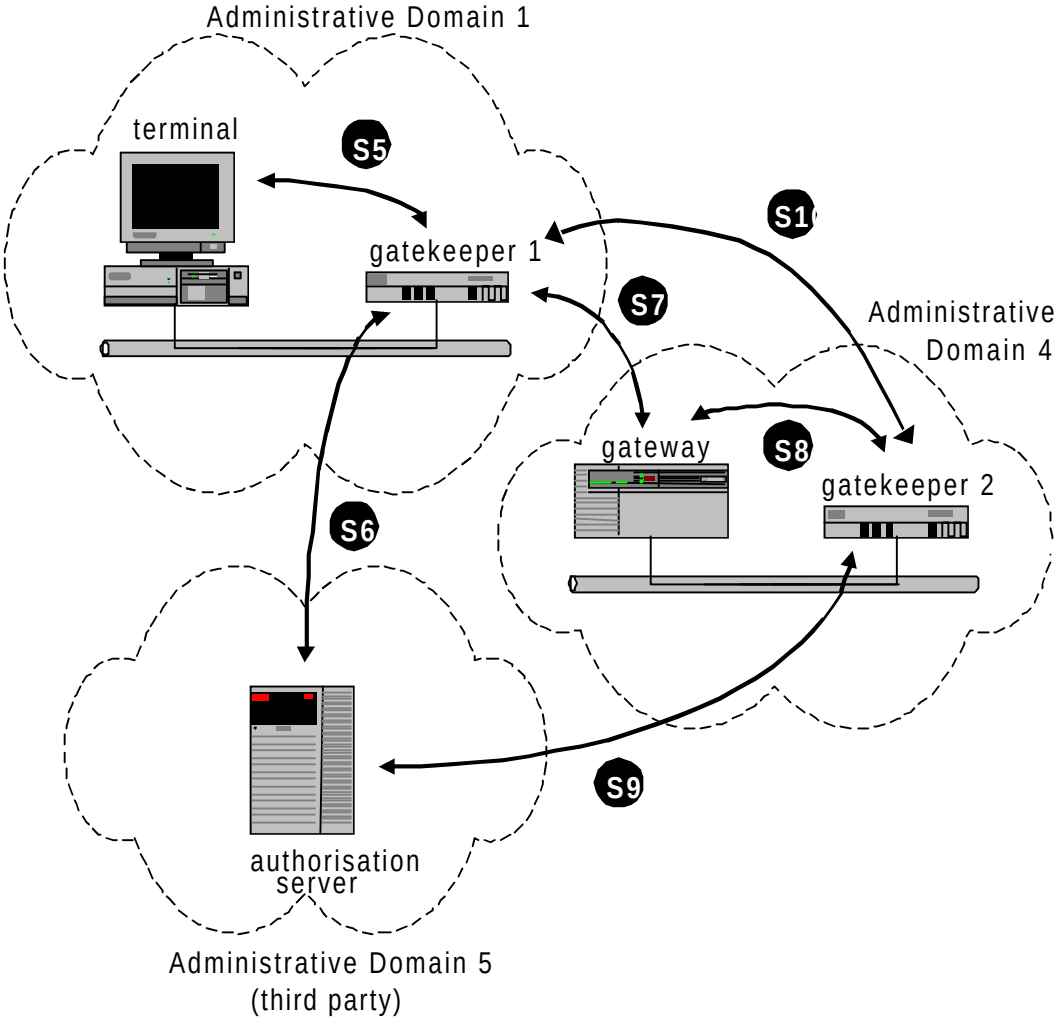


Figure 8: Security information flows for Operator authentication and authorization

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.

9.2.3 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.

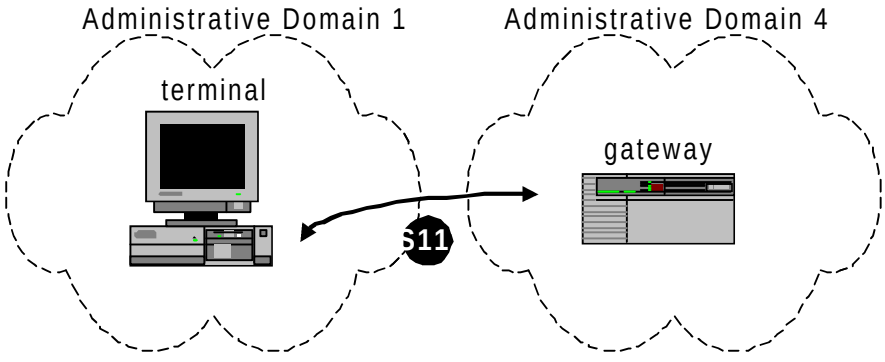


Figure 9: Security information flows for call signalling

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]).

9.2.4 Call Activity

Once a call is established and active, it may require security services such as media stream privacy. Figure 11 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.

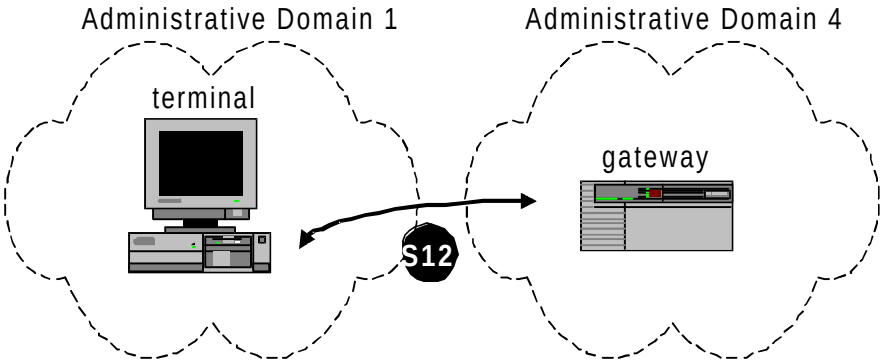


Figure 10: Security information flows for call activity

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.

9.2.5 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.

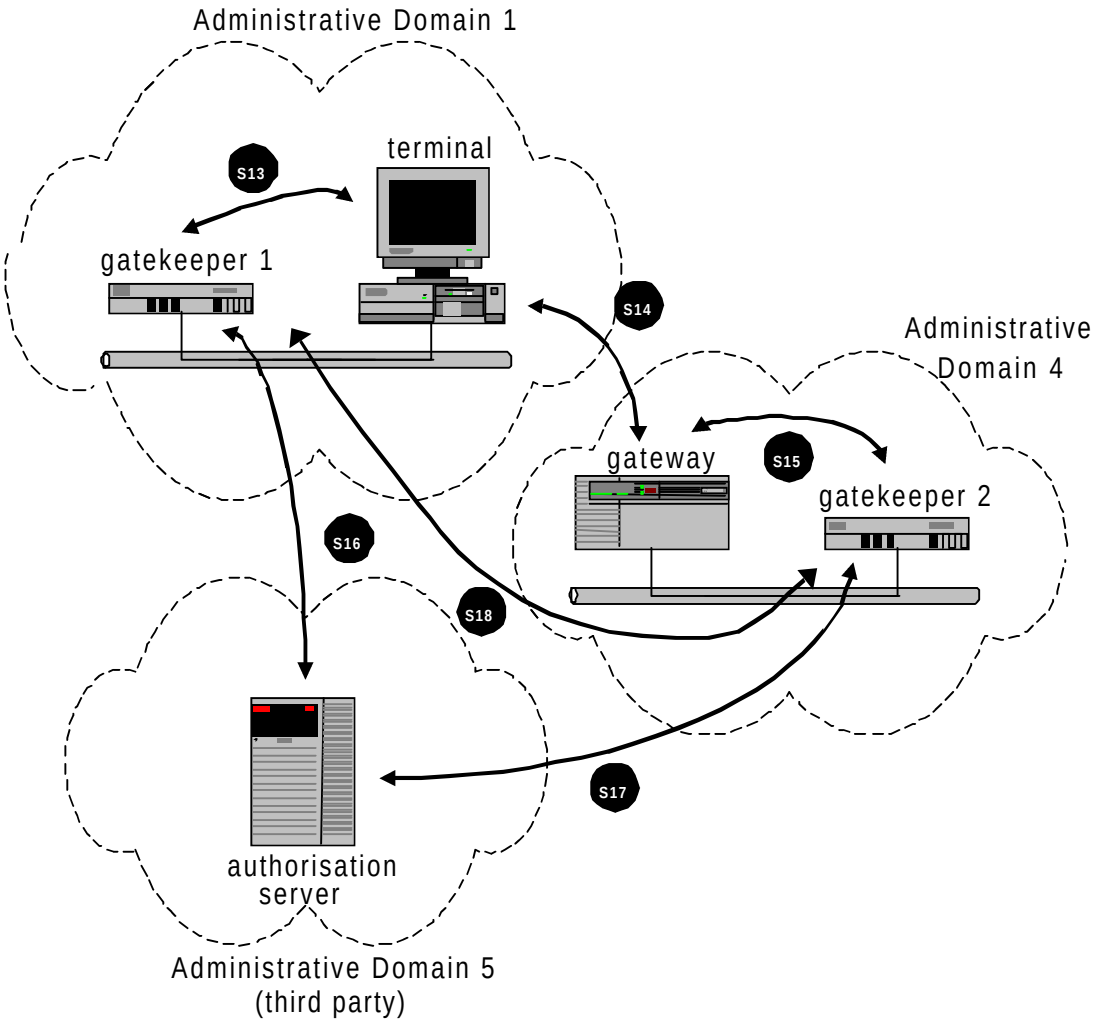


Figure 11: Security information flows for call clearing

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.

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

The requirements concerning operations, administration, and management of TIPHON systems will be within scope of future issues of the present document.

Annex A (informative): Use cases for the architecture.

This informational annex contains several illustrations of possible implementations of the architecture. These illustrations not meant to be exhaustive. Other combinations of elements are possible and allowed.

A.1 Illustration 1

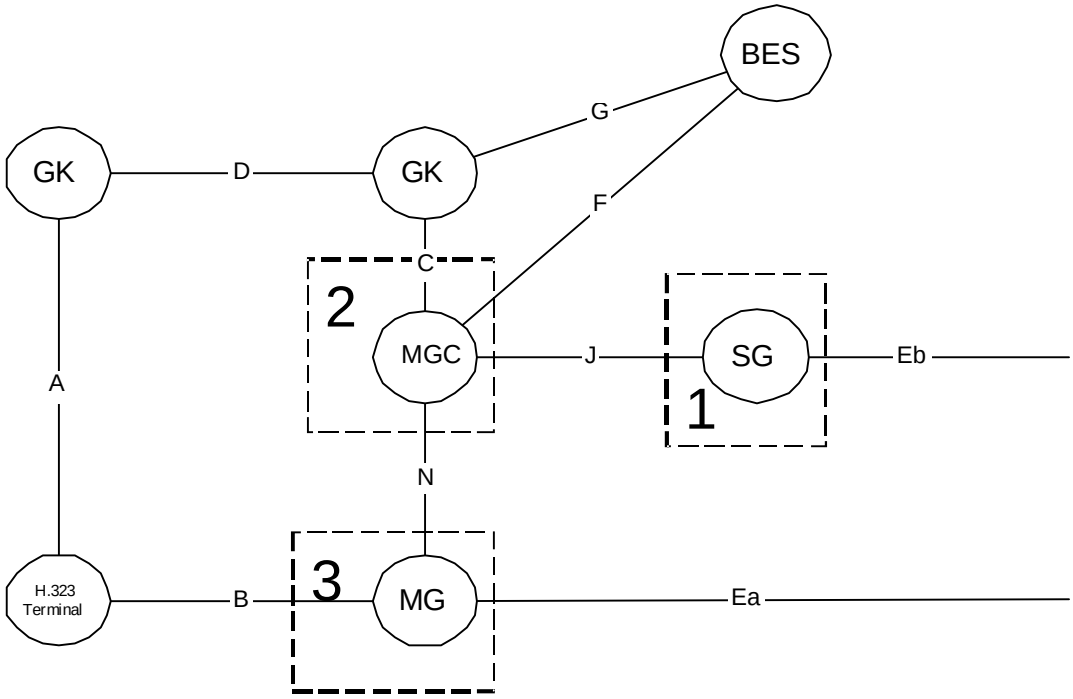


Figure A.1: Illustration 1

The implementation pictured in Figure A.1 shows three boxes. Box 1 is a Signalling Gateway which connects with the SCN SS7 network. The SG function allows concentration of signalling links, and conservation of SS7 point codes.

Box 2 is a Media Gateway Controller which communicates with the SCN via the Signalling Gateway, and to the IP network via a Gatekeeper. The MGC function frees the call processing and service intelligence from the physical media ports. The MGC function can run on general purpose computers, and need not be replaced should a new media port type be introduced into the service provider's network.

Box 3 is a Media Gateway with SCN circuits and IP connectivity. The Media Gateway contains the physical ports that are manipulated by the Media Gateway Controller. As new types of ports are introduced into the service provider's network, new Media Gateways can be added without impacting the existing Media Gateways.

In Figure 2, the GK function must be provided by some additional equipment which connects with the Media Gateway Controller. The equipment described in Figure A.1 has no capability to process inband signalled trunks, and must receive all signalling information from the one Signalling Gateway.

A.2 Illustration 2

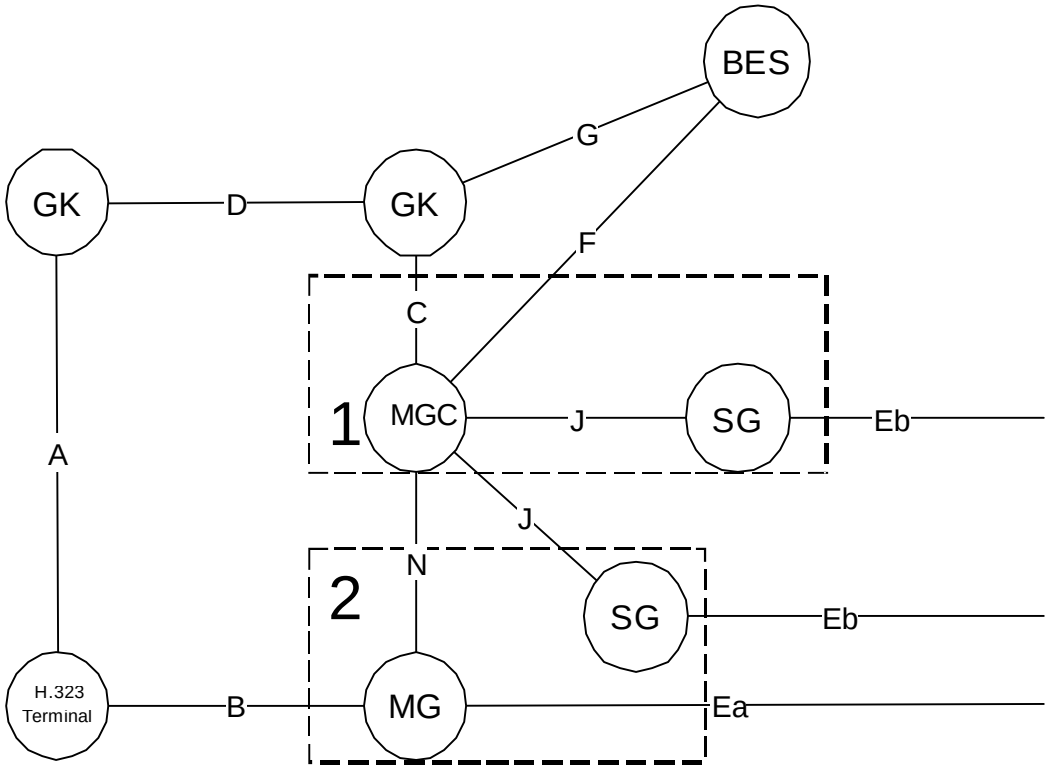


Figure A.2: Illustration 2

The implementation pictured in Figure A.2 shows two boxes. Box 1 is a combination of Media Gateway Controller and Signalling Gateway. This box has an internal connection between the Signalling Gateway and the Media Gateway Controller which may or may not comply with any standard. Since the functions are combined inside the box, there is no need for this connection to be visible outside of this box. The Signalling Gateway function communicates with the SCN SS7 signalling network.

Box 2 is a comined Signalling Gateway and Media Gateway with SCN connections and IP connectivity. The SCN connections supported are those where the signalling information is carried by the same physical medium as the user information, e.g. PSTN. The Media Gateway contains physical ports that are manipulated by the Media Gateway Controller. The Signalling Gateway located inside the box supports the signalling messages transmitted along with the bearer channels.

NOTE: This illustration (and others below) identify a Signalling Gateway co-located with the Media Gateway in addition to a second Signalling Gateway. The second Signalling Gateway need not be present in implementations that only support the case where the signalling information is carried by the same physical medium as the user information.

As in the previous illustration , the GK function must be provided by some additional equipment which connects with Box 1.

A.3 Illustration 3

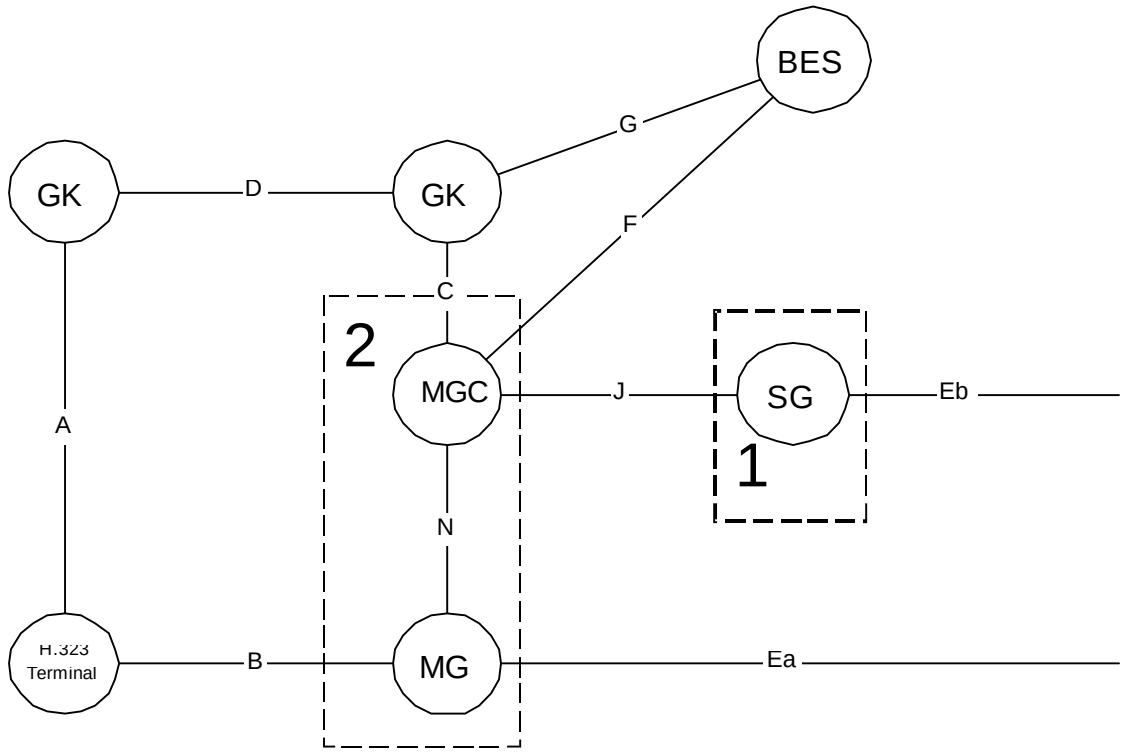


Figure A.3: Illustration 3

The implementation pictured in Figure A.3 shows two boxes. Box 1 is a Signalling Gateway which connects with the SCN SS7 network.

Box 2 is a combination of Media Gateway Controller and Media Gateway. This box has an internal connection between the Media Gateway Controller and the Media Gateway which may or may not comply with any standard. Since the functions are combined inside the box, there is no need for this connection to be visible outside of this box.

As in the previous illustrations, the GK function must be provided by some additional equipment.

A.4 Illustration 4

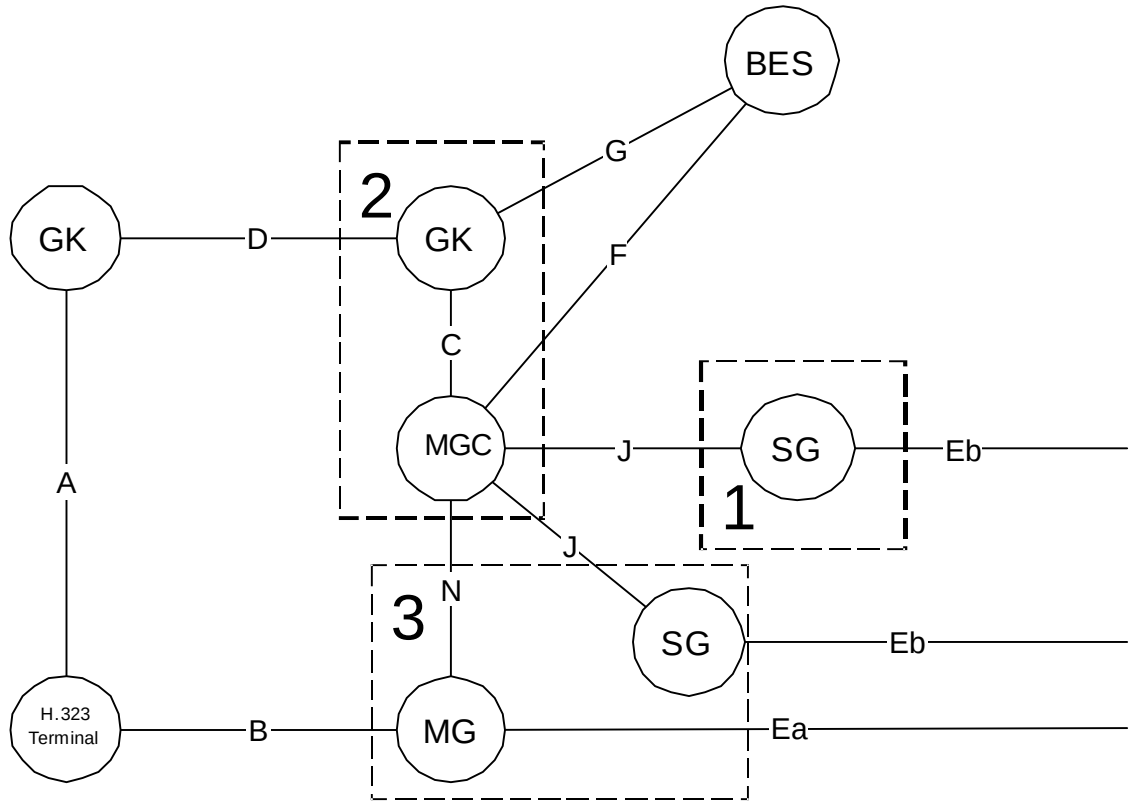


Figure A.4: Illustration 4

The implementation pictured in Figure A.4 shows three boxes. Box 1 is a Signalling Gateway which connects with the SCN SS7 network.

Box 2 is a combination of Media Gateway Controller and Gatekeeper. This box has an internal connection between the GK and the Media Gateway Controller which may or may not comply with any standard. Since the functions are combined inside the box, there is no need for this connection to be visible outside of this box. The GK function communicates with other GK boxes and with H.323 Terminals.

Box 3 is a combined Signalling Gateway and Media Gateway with SCN connections and IP connectivity. The SCN connections supported are those where the signalling information is carried by the same physical medium as the user information, e.g. PSTN. The Media Gateway contains physical ports that are manipulated by the Media Gateway Controller. The Signalling Gateway located inside the box supports the signalling messages transmitted along with the bearer channels.

A.5 Illustration 5

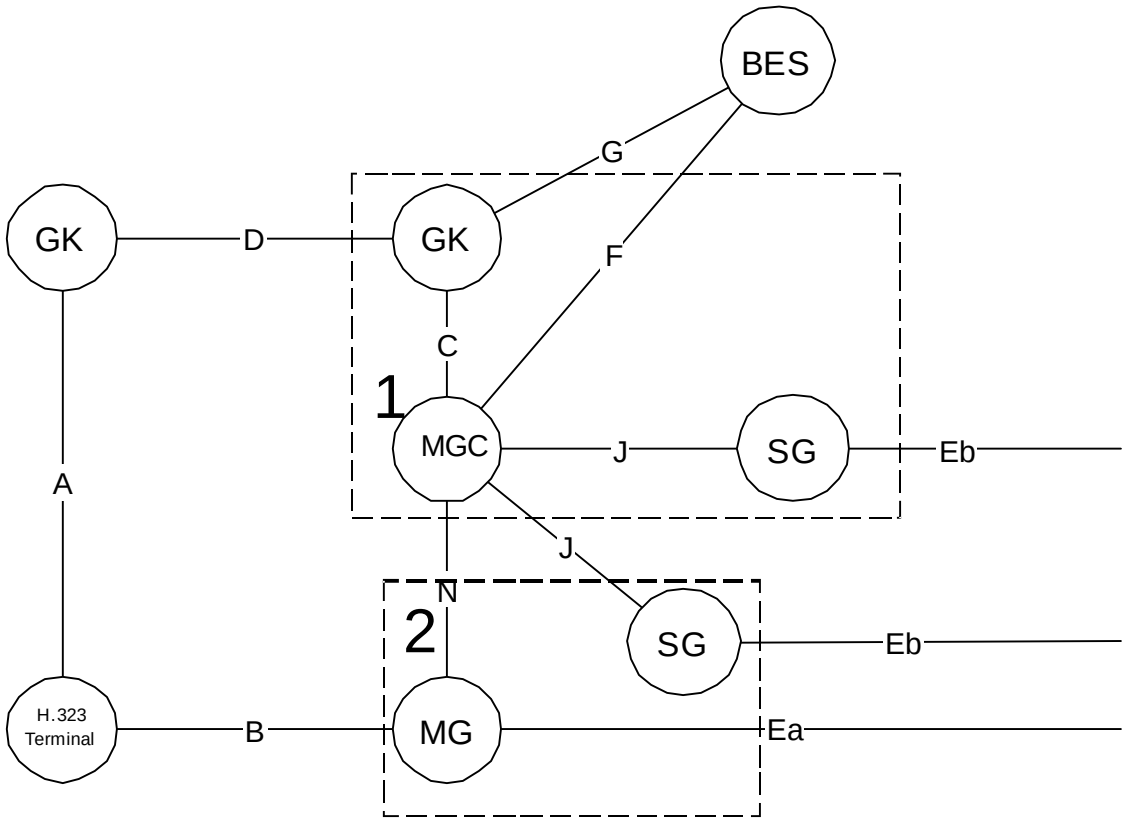


Figure A.5: Illustration 5

The implementation pictured in Figure A.5 shows two boxes. Box 1 is a combination of Gatekeeper, Media Gateway Controller and Signalling Gateway. This box has two internal connections between the GK and Media Gateway Controller, and between the Signalling Gateway and the Media Gateway Controller. Either or both of which may or may not comply with any standard. Since the functions are combined inside the box, there is no need for this connection to be visible outside of this box. The SG function communicates with the SCN SS7 signalling network, the GK function communicates with H.323 network elements, and the Media Gateway Controller communicates with the Media Gateway.

Box 2 is a combined Media Gateway and Signalling Gateway with SCN connections and IP connectivity. The SCN connections supported are those where the signalling information is carried by the same physical medium as the user information, e.g. PSTN. The Media Gateway contains physical ports that are manipulated by the Media Gateway Controller. The Signalling Gateway located inside the box supports the signalling messages transmitted along with the bearer channels.

Annex B (informative): Example Call flows for the reference architecture

The following examples show call establishment from an H.323 terminal and also from a terminal in an SCN. In these examples, the SCN protocol used is ISUP and the fast call setup mechanism is used.

B.1 H.323 originated call setup

In Figure B.1 is depicted an example of a call being setup from a H.323 terminal (scenario 1).

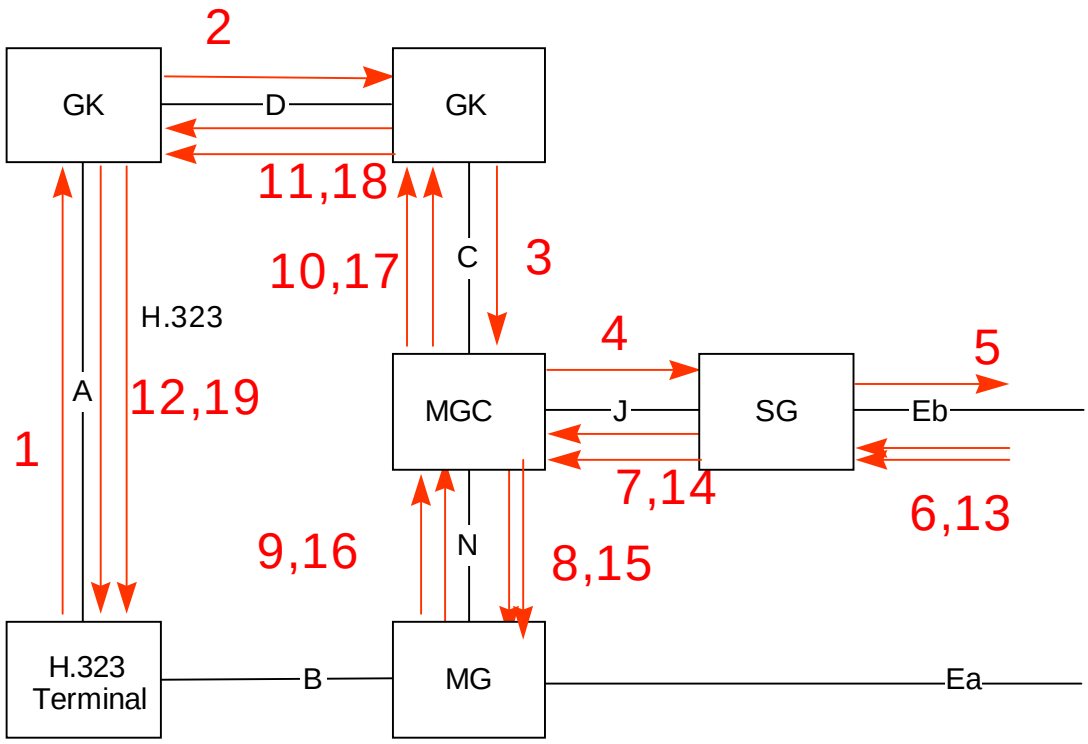


Figure B.1: H323 initiated call setup

The steps are as follows:

1) H.225.0 setup;
2) inter-zone H.225.0 setup (assumes that all 800 numbers are forwarded to the other gatekeeper);
3) H.225.0 setup to appropriate MGC;
4) setup to Signalling Gateway;
5) Initial Address Message over ISUP;
6) ISUP Address Complete;
7) ack;
8) configure MG (including info on RTP ports of call originator);
9) ack (includes RTP ports for MG);
10) to 12) ack + info on media termination (H.225.0 Proceeding);

13) ISUP Answer Message;

14) answer message forwarded;

15) activate path in MG (give trunk line channels?);

16) ack;

17) to 19) H.225.0 Connect.

At this point the call is connected end-to-end and media is streamed.

B.2 SCN originated call setup

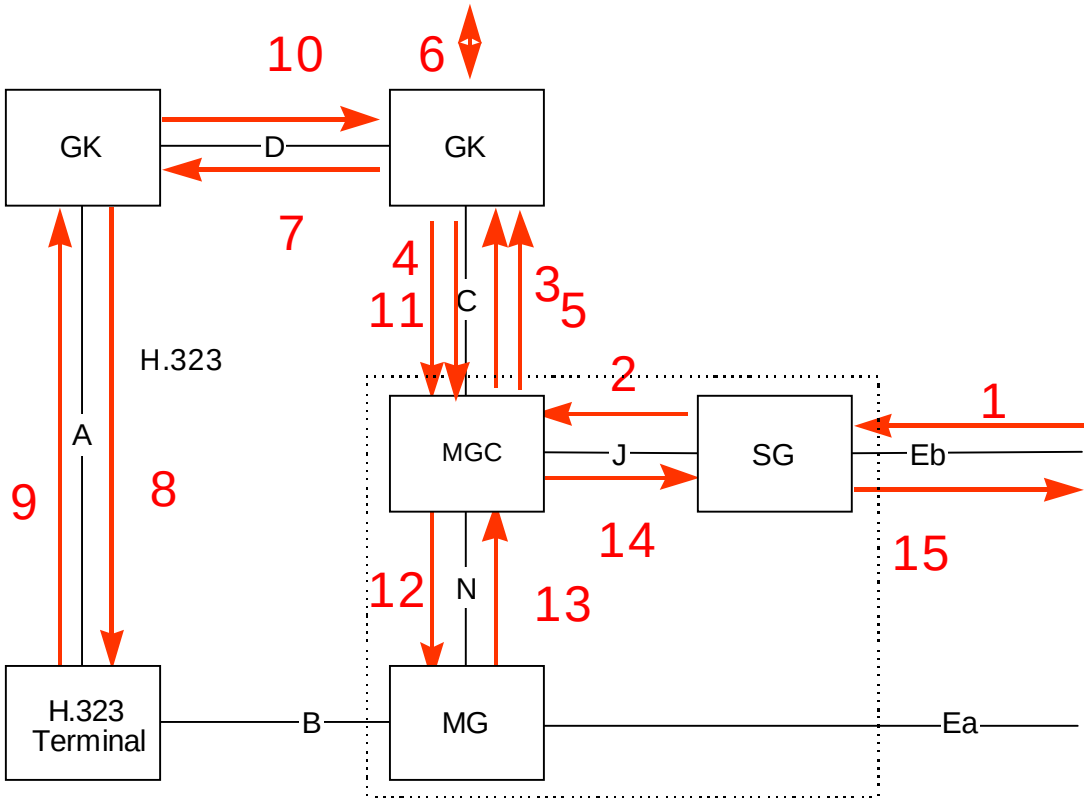


Figure B.2: SCN originated call setup

The scenario assumes setup initiated from the SCN (scenario 2) (see Figure B.2).

1) ISUP Initial Address message;
2) setup forwarded;
3) admission request (RAS);
4) admission confirm;
5) H.225.0 setup;
6) map E.164 number to H.323 alias;
7) H.225.0 (inter zone) setup to other GK;
8) H.225.0 setup to Terminal (assume v2);
9) Terminal CONNECT;

10), 11) CONNECT forwarded;

12) media gateway is told to forward the media stream (tells IP address, encoding) and trunk ID on PSTN side;

13) MG acks and gives its own RTP ports;

14) CONNECT;

15) ISUP CON.

At this point the call is connected end-to-end and media is streamed

B.3 800 number resolution

Figure B.3 is an example of the use of an IN back-end service, in this case a dip into the 800 database.

1) Query to find routing address of recipient (or rather his provider) to find appropriate MGC - this query may result in for example:
   - IN dip (INVOKE over TCAP).
   - RETURN RESULT (over TCAP) (gives the identity of the carrier).
2) Response to the query.

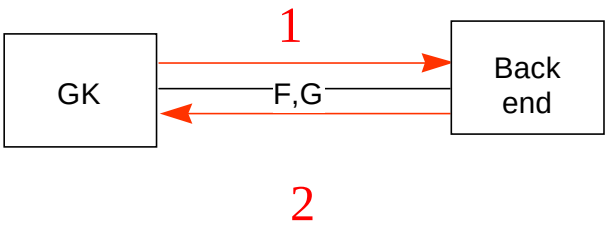


Figure B.3: Example query to 800 database

History

Document history		
V0.4.2	February 1999	Publication

ISBN 2-7437-2869-8
Dépôt légal : Février 1999