International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.235.9

(09/2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Systems aspects

H.323 security: Security gateway support for H.323

ITU-T Recommendation H.235.9

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	**H.230–H.239**
Communication procedures	H.240–H.259
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND AND TRIPLE-PLAY MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation H.235.9

H.323 security: Security gateway support for H.323

Summary

This Recommendation defines a method for the discovery of Security Gateways in the signalling path between communicating H.323 entities, and for sharing of security information between a gatekeeper and the SGs in order to preserve signalling integrity and privacy.

Source

ITU-T Recommendation H.235.9 was approved on 13 September 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Gateway, security, signalling.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Introduction

The use of Firewalls and/or Network Address Translation devices to provide traffic security between network regions under different administrative controls creates problems for telephony signalling protocols that must exchange network addresses for signalling and media exchange.

ITU-T Rec. H.235.5 introduces a framework by which an endpoint and its gatekeeper, or two gatekeepers, can use the initial RAS messages to negotiate a set of strong-shared secrets between them, and use those secrets to encrypt selected parts of subsequent RAS and call signalling messages and to authenticate those messages. The method applies to gatekeeper-routed signalling only. Similar methods and security profiles are defined by ITU-T Recs H.235.1, H.235.2 and H.235.3. This security can come into conflict with Application Level Gateways (ALGs) which interconnect network realms and manipulate the signalling and media transport addresses carried in the H.225.0 RAS and/or call signalling messages. Such changes in the message will cause the message authentication check to fail at the destination.

This Recommendation describes a simple means by which the gatekeeper may be informed of the ALGs in a signalling path, and may share the negotiated signalling authentication key with those ALGs. This will permit the ALGs to manipulate non-private data, particularly transport addresses, in the signalling messages, and then authenticate the result before passing the modified messages onward. Such devices are referred to as Security Gateways (SGs) in the subsequent text. This technique retains the end-to-end privacy of any encrypted elements in the signalling.

ITU-T Recommendation H.235.9

H.323 security: Security gateway support for H.323

1 Scope

This Recommendation is usable by any gatekeeper and endpoint using the H.225.0 RAS protocols, with one or more intervening Security Gateways with the prescribed behaviour.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.

– ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile*.

– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile*.

– ITU-T Recommendation H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.

– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication*.

– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems*.

2.2 Informative references

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

3 Definitions

This Recommendation defines the following terms:

3.1 application level gateway: A protocol-aware device that interconnects two or more network regions which is able to interpret and modify the application level protocols to provide transport address translations and other functions. An ALG may provide transport level NAT and firewall functions internally, or may control them externally.

3.2 local address: A transport address within a local address realm.

3.3 media gateway: A device which interconnects two or more network realms and which can be controlled by another device (e.g., an SG) to provide controlled media flows between realms. The MG is effectively a programmable NAT/firewall operating at the transport layer and below.

3.4 network address translation: The operation of mapping network transport addresses from one network realm to another.

3.5 pinhole: A flow path through an SG (or a media gateway under its control) by which packets or messages are permitted to move from one realm to another. A pinhole is typically characterized by four transport addresses (the realm A source address, the SG realm A address, the SG realm B address, and the realm B destination address), and other characteristics such as transport protocol and directionality. The source address may be unspecified, e.g., for a listen port.

3.6 realm: A network region which shares a common network address space; by presumption, different realms use incompatible, conflicting, or private address spaces.

3.7 security gateway: A device installed between two or more IP network regions in order to perform security functions such as the validation or restriction of packet flows and the mapping of transport addresses between network regions. For this Recommendation, it is assumed that the Security Gateway is an ALG knowledgeable of H.323 signalling protocols.

4 Abbreviations

This Recommendation uses the following abbreviations:

ALG Application Level Gateway

GCF GatekeeperConfirm

GK Gatekeeper

GRJ GatekeeperReject

LCF LocationConfirm

LRQ LocationRequest

MG Media Gateway

NAT Network Address Translation

OID Object Identifier

RAS Registration, Admission and Status

SG Security Gateway

UDP User Datagram Protocol

5 Conventions

This Recommendation defines various object identifiers (OIDs) for signalling security capabilities, procedures or security algorithms. These OIDs relate to a hierarchical tree of assigned values that may origin from external sources or are part of the ITU-T maintained OID tree. Those OIDs that are specifically related to ITU-T Rec. H.235 have the following appearance in the text:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**} where **V** symbolically represents a single decimal digit denoting the corresponding version of ITU-T Rec. H.235; e.g., 1, 2, 3 or 4. **N** symbolically represents a decimal number uniquely identifying the instance of the OID and thus, the procedure, algorithm or security capability.

Thus, the ASN.1 encoded OID consists of a sequence of numbers. For convenience, a textual mnemonic shorthand string notation for each OID is used in the text such as "OID". A mapping is

given that relates each OID string with the ASN.1 sequence of numbers. Implementations conforming to ITU-T Rec. H.235 shall use only the ASN.1 encoded numbers

Basic Assumptions

This Recommendation considers an IP network model in which multiple network regions, called realms, are interconnected by devices called Security Gateways (SGs) which are H.323 protocol aware, and which are designed to control information flows between the network realms they interconnect. The SGs are expected to examine signalling messages flowing between realms, insure their validity, and extract transport address information being exchanged, and use that transport information to construct appropriate flow paths between the realms, and to modify the transport addresses as appropriate for the realm to which the message is forwarded. The SGs must insure the signalling paths flow through themselves, of course, but they may control another device to support any media flows that are established. The control protocol between the SG and the "media gateway" is not specified by this Recommendation.

In order to make the services of a gatekeeper in one realm available to endpoints or gatekeepers in another realm, an SG may provide a gatekeeper discovery address in each realm it serves in which there is no known gatekeeper. The SG would then forward any discovery message received on one of those addresses on toward the actual gatekeeper after performing any necessary processing of the H.323 message. An example configuration is illustrated in Figure 1, which shows a gatekeeper serving endpoints in multiple network realms.

In effect, the Security Gateways must represent the gatekeeper in each of the realms they serve (except, of course, the realm in which the gatekeeper resides, e.g., realm A for gatekeeper A in the diagram). SG B provides discovery addresses for both gatekeepers in the figure, thus it provides a gatekeeper-to-gatekeeper path for LRQ/LCF signalling. Note also that an SG need not provide access to every gatekeeper in every realm. For example, in Figure 1, SG A might be configured to supply a discovery address in realm B only for gatekeeper A.

It is assumed that each gatekeeper knows a unique name for each SG in the system, and that the gatekeeper and each SG also share a cryptographically strong secret that may be used to communicate securely between them. The manner in which these identities, and the corresponding keys, are negotiated or exchanged is discussed below, but is not the main subject of this Recommendation. The shared secrets should be unique per SG/gatekeeper pair. It is assumed that the SGs will modify the RAS and call signalling addresses exchanged to insure that the RAS and call signalling traffic passes through them.

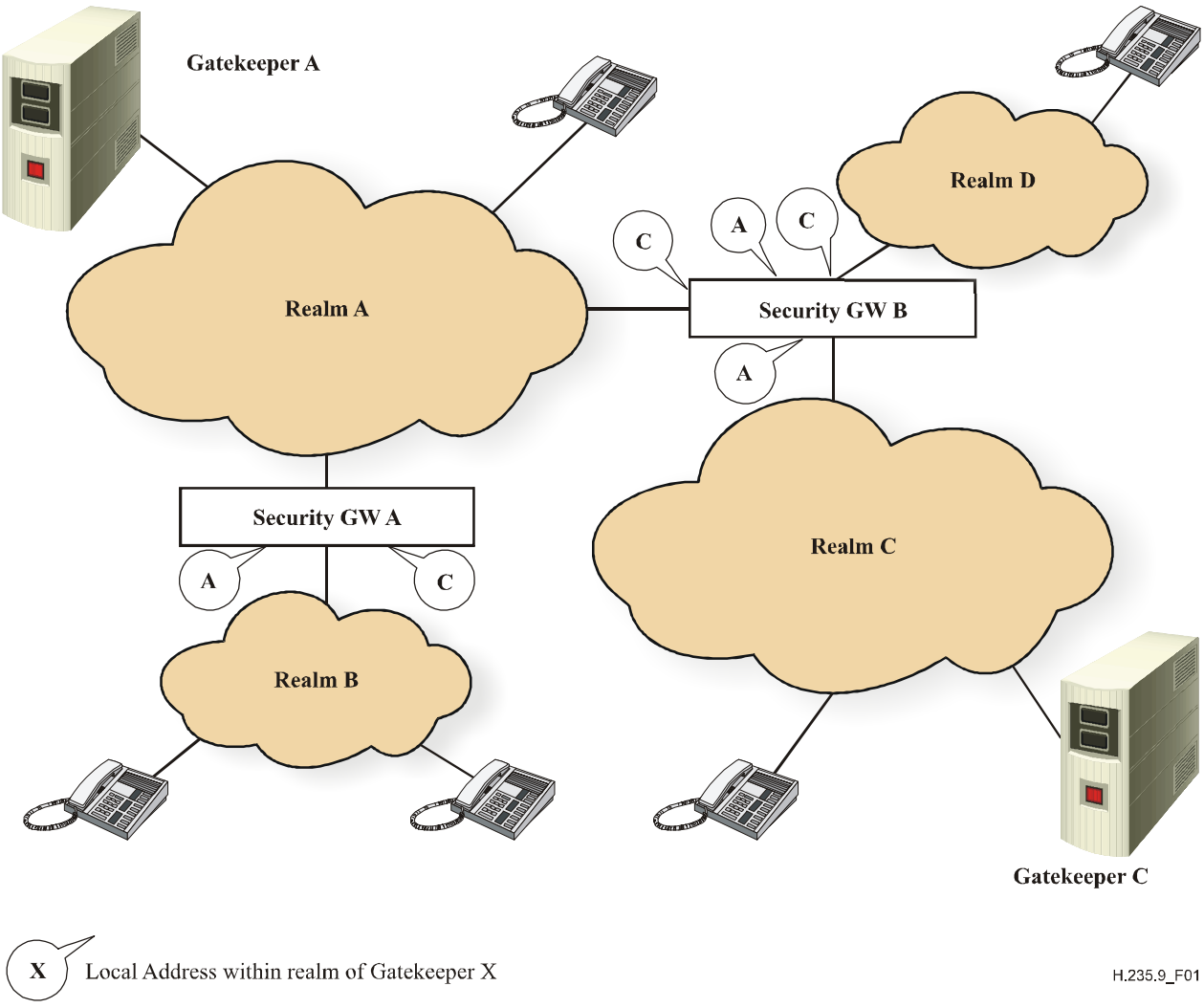


Figure 1/H.235.9 – Security gateway configuration

In addition, the means by which routing and/or address translation for the initial discovery process is established is not the main subject of this Recommendation, but is discussed below. Subsequent address establishment, along with any required translations, are presumed to be carried out as part of the operation of the SGs.

6 Basic operation

The following description assumes that each SG present in the system has registered with each gatekeeper it is expected to serve. The details of how this may be done are described later. For the basic operation, it is assumed that the SG has identified itself to each gatekeeper, shares a unique, strong secret with each gatekeeper, and provides one or more "local" gatekeeper discovery addresses for each gatekeeper. The details of SG registration will be discussed in a later clause. The following describes how the SGs participate in endpoint registration in order to obtain access to the end-to-end authentication key negotiated between the GK and the endpoint.

6.1 Endpoint gatekeeper discovery

When an endpoint sends a GRQ to a gatekeeper discovery address, and the GRQ passes through an SG enroute to one or more gatekeepers, the SG may add a **ClearToken** to the GRQ.**token** element as it manipulates addresses within the GRQ. This **ClearToken** will be identified as an SG-id token (via its **tokenOID**), and will contain an identification string that uniquely identifies the SG. The SG

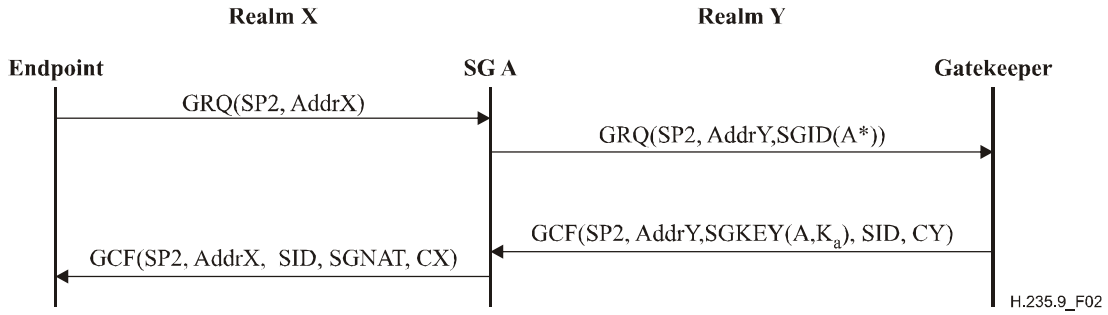
should remove, from the GRQ's **authenticationCapability** profile, any particular **AuthenticationMechanism** (e.g., TLS in RFC 2246 and RFC 3546 or IPsec in RFC 2401) whose message authentication procedure it is unable to support. This will insure that the gatekeeper will select a profile that is compatible with the SG. The first SG to receive the GRQ shall include an element identifying the discovery address at which it received the GRQ from the endpoint.

It is implicitly assumed that each SG will manipulate any signalling address fields within the GRQ and subsequent RAS messages to insure that all signalling messages flow through the SG for address processing.

6.2 Endpoint authentication key distribution

When the GRQ reaches the gatekeeper (GK), the gatekeeper will process the GRQ, including the SG-id token. Assuming the GK will act as the endpoint's gatekeeper, it will prepare to send a GCF back to the endpoint. The GK will then include, in the GCF message, the chosen **AuthenticationMechanism**, along with an SG-key **ClearToken** (identified by its **tokenOID**) for the SG identified by the SG-id token received. This key token will include the identification of the SG, the identification of the GK, an initialization vector, and the session authentication key encrypted using the IV, and the secret shared between the SG and the gatekeeper. The encryption algorithm shall be negotiated during SG registration, or pre-provisioned.

As the GCF is passed back along the path to the endpoint, it passes through the SG that supplied the SG-id token. The SG shall parse the message to obtain the session ID and its own key token. It shall then decrypt the session authentication key and use it to authenticate the received message. If the message is authentic, the SG will manipulate any transport addresses as appropriate, then rebuild the message without its own SG-key token, insert an SG-NAT token if one is not already present, then authenticate the rebuilt message and send it on. The session ID and authentication key shall be preserved for use with subsequent RAS and call signalling messages for that session. The basic sequence through a single SG is illustrated in Figure 2. Note also that the SG must prepare any pinholes as inferred from the GCF (e.g., a RAS pinhole and alternate GK address pinholes.)



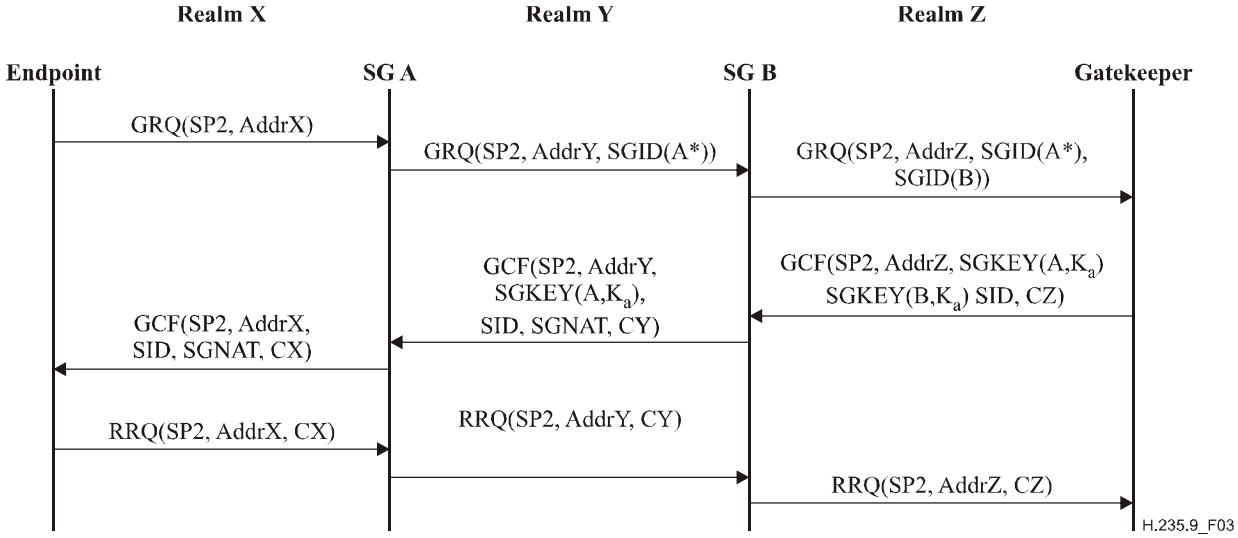
SP2 = H.235.5 security profile
Addrx = addresses in the x realm
SGID(A*) = SG-id ClearToken identifying presence of SG A
(* indicates SGID includes discovery address used by GRQ.)
SID = session ID (assigned by Gatekeeper)
K_a = message authentication key for SID
SGKEY(A, K_a) = SG-key ClearToken with K_a encrypted under A's secret key.
SGNAT = SG-NAT ClearToken
Cx = message checksum (computed using negotiated K_a) in realm x

Figure 2/H.235.9 – Basic SG traversal exchange

This scheme easily extends to a series of SGs between the endpoint and the gatekeeper. Each SG adds its own ClearToken to the GRQ as it passes through, and strips off its own reply ClearToken from the GCF as it passes back from the Gatekeeper to the endpoint. The first SG in the path back

to the endpoint shall insert the SG-NAT token in the GCF. Figure 3 shows this operation. The processing of subsequent RAS messages is illustrated by showing the transformation of transport addresses in an RRQ message, and the recomputed checksum.

A similar sequence may be carried out in an LRQ/LCF exchange, using the same message elements, and the results may be used to process and authenticate subsequent signalling messages for that session.



SP2 = H.235.5 security profile
Addrx = addresses in the x realm
SGID(A*) = SG-id ClearToken identifying presence of SG A
(* indicates presence of discovery address used by endpoint.)
SID = session ID (assigned by Gatekeeper)
K_a = message authentication key for SID
SGKEY(A, K_a) = SG-key ClearToken with K_a encrypted under A's secret key.
SGNAT = SG-NAT ClearToken
Cx = message checksum in the x realm

Figure 3/H.235.9 – Two-level SG traversal exchange

6.3 Address manipulation

As each H.225.0 or H.245 signalling message passes through it, the SG must examine and replace any transport addresses carried therein so that they are valid within the next realm through which the message will travel. This may require the SG to establish new flow pinholes to support the associated signalling and/or media flows these addresses are meant to establish. Note that some addresses represent listen ports that must be opened "just in case"; a fully-specified pinhole will be created when/if a packet arrives at the listen port.

Each SG may examine each received destination transport address to see if it actually represents a destination address on that SG. Consider the example realm configuration and media paths in Figure 4. A media stream from an endpoint in realm B to an endpoint in realm C must flow through SGs B and C as illustrated by the flow labelled "1". Without any special processing by SG B, a media stream between two endpoints in realm B would follow an equivalent path up to realm A and back to realm B, as illustrated by the flow labelled "2". Now, if SG B recognizes that the source and destination addresses supplied for the flow in realm A are actually addresses on SG B, then it can "short-circuit" the flow in either of two ways: it can route the flow internally, as illustrated by flow "3" (shown on SG C for clarity), or, if it recognizes that both endpoints reside in realm B, it can substitute realm B endpoint addresses to route the flow directly between the endpoints as shown by flow "4". Note that the "endpoint" addresses as seen by SG B might actually be addresses on an SG

(call it D) connecting to another realm. After SG B modifies the addresses to perform "direct" routing between addresses on SG D, SG D may then short-cut the flows in the same manner.

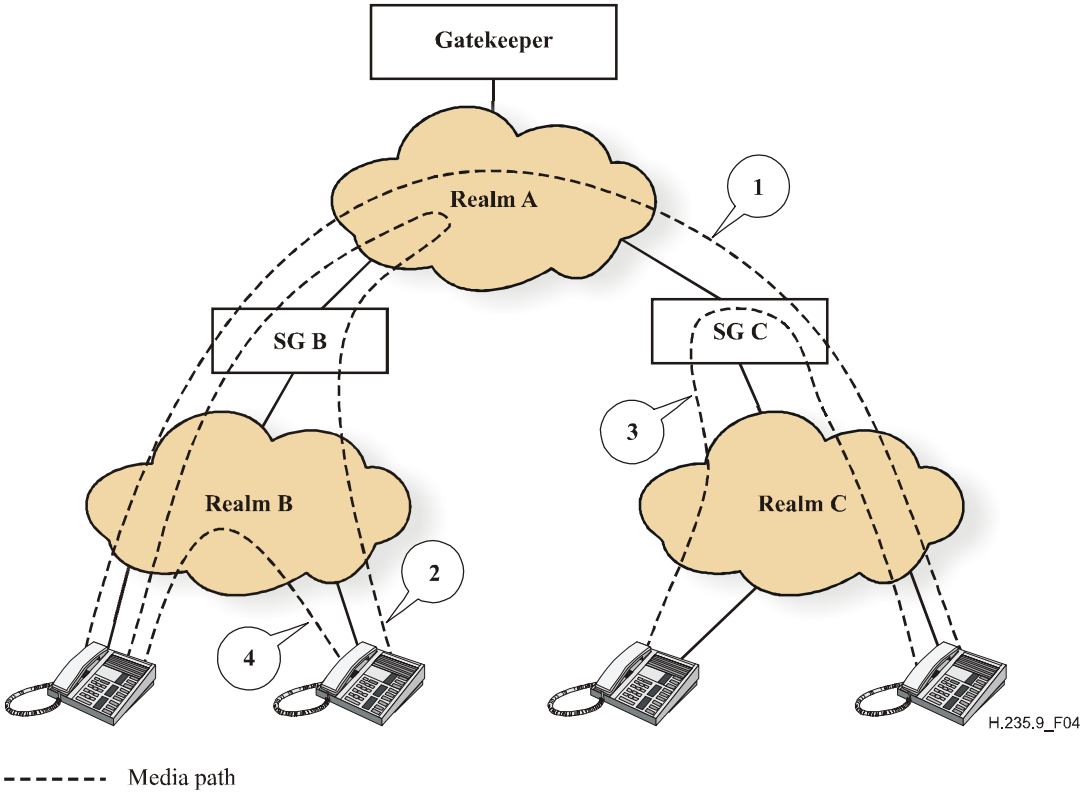


Figure 4/H.235.9 – Media paths

One configuration that is not handled by this scheme is the case where one region gains access to another region via more than one SG. If an endpoint registers and signals through one SG, and another endpoint in the same region signals through a second SG, then it will be difficult for either SG to discover that both endpoints are in the same realm, or what addresses to use for the endpoint which signals through the other SG. To avoid this problem, it is convenient to employ a single SG that is capable of processing the expected level of signalling; the media flow processing load can be relegated to separate media gateways under control of the SG.

7 Signalling details

Support for this capability is most effectively identified via a standard object identifier (OID) in the applicable clear tokens. In the following, these tokens will be referred to as SG tokens. This permits the feature to be ignored by any receiving gatekeeper (or intervening gateway or other device that does not participate). The assigned OID will be used to identify **ClearToken**s which carry the following elements:

- **tokenOID** – set to the OID assigned to this feature, call it "SG1", see clause 11.
- **generalID** – if present, set to the name of the SG to which this **ClearToken** is directed (used in the SG-key token).
- **sendersID** – set to the name of the SG which created this **ClearToken** (used in the SG-id token).
- **profileInfo** – contains the specific information carried by this **ClearToken**, as specified in Table 1.

Table 1/H.235.9 – Profile elements for SG discovery

Element name	ElementID value	Element type (length)	Element description
Token Type	1	integer	0 = SG-id token 1 = SG-key token 2 = SG-NAT token 3 = SG-register token
Encrypted Key	2	octets (16 for SP2)	Session authentication key from the indicated security profile, encrypted under the secret shared between the specified SG and the GK. Sent in SG-key token. The necessary IV for decryption is specified in ProfileElement.paramS.
ServedRealm	3	name	Name of Realm in which SG can/should provide a gatekeeper discovery address

8 SG configuration considerations

The procedures described in this Recommendation depend on some means for the SGs in the network to discover paths to the gatekeeper(s) whose services are to be made accessible to users in different realms of the network. Each SG must be able to contact its gatekeeper (or gatekeepers) in one realm, and provide access to those gatekeepers from endpoints (or other gatekeepers) in the other realm. For example, in Figure 3, SG B accesses the gatekeeper in realm Z. It can provide access to the gatekeeper for elements in realm Y. Thus, SG A can access the gatekeeper through SG B. Once SG B has access to the gatekeeper, it can provide access for parties in realm X. This suggests the use of a discovery protocol such as RAS by the SGs themselves. These procedures could also be used to identify each SG to each gatekeeper it can access, and to negotiate (a set of) keys to protect the user signalling exchanges.

8.1 SG registration

An SG may serve as a representative, within a realm, of a gatekeeper in another realm to which the SG has access. For example, in Figure 1, SG A can provide a representation (a discovery address) in realm B for the gatekeeper in realm A, once it knows the gatekeeper's discovery address in realm A. This technique can be extended to several levels of SGs; as each SG discovers a gatekeeper (or a representative) it can provide a discovery address for that gatekeeper in one or more new realms, at which point SGs connected to that realm can discover those new addresses.

SGs shall use H.225.0 RAS procedures to discover and register with gatekeepers in any realm to which they want to provide service as a Security Gateway. An SG shall identify itself as a **gateway** endpoint type. The SG may specify protocol support for H.323 if it wishes to specify supported prefixes and/or bandwidth limitations, but this is not required. Standard security procedures such as those described in ITU-T Recs H.235.1, H.235.2, H.235.3 and H.235.5 shall be used to authenticate the SG to the gatekeeper and to negotiate secure shared secrets to be used in the procedures described below. H.235.1, H.235.2, H.235.3 and H.235.5 procedures can pass through other security gateways supporting this Recommendation. The SG must also include an SG-register ClearToken in the RRQ it sends toward the gatekeeper. This token serves to identify the gateway as an SG, and it shall contain a **ServedRealm** element for each new realm the SG will serve. Each element represents a potential new gatekeeper discovery address in its respective realm. Each SG may be configured to restrict the realms to which it will provide discovery addresses for a gatekeeper. For example, in Figure 1, SG B might be configured to not provide a discovery address for gatekeeper C in realm D, thus forcing endpoints in realm D to register to gatekeeper A. Insofar

as the SG does not itself make or receive calls, it need not supply a call signalling address during its registration; it may provide an empty SEQUENCE for **callSignalAddress** in the RRQ. The gatekeeper shall respond in kind in **callSignalAddress** of the RCF.

The gatekeeper shall indicate which realm(s) for which the SG may provide service by returning, in the RCF, an SG-register token containing one or more of the **ServedRealm** elements from the SG's RRQ. Once registration is complete, the SG shall open a listen socket for a gatekeeper discovery address in each indicated realm. Mechanisms outside this Recommendation may be used to announce this discovery address within the realm. The gatekeeper may choose to use the discovery addresses supplied by the SG in a list of alternate addresses.

Any RAS security profile may be used, so long as the SGs are permitted to read and manipulate the signalling and media transport addresses exchanged and may re-authenticate the message.

The gatekeeper can make use of SG realm information to map network regions and connectivity, and to authenticate the SG. The gatekeeper should provide information back to the SG:

- The gatekeeper's credentials.
- Registration address(es) the SG may use to relay RAS requests from endpoints in the region(s) it serves (i.e., the GK can decline to support endpoints in one or more regions served by the SG.).

One important result of successful SG registration should be a strong secret key shared between the SG and the gatekeeper from which encryption and/or authentication keys may be derived. The authentication key may be used to authenticate the SG registration scheme, and the encryption key should be used during endpoint registrations to encrypt the endpoint session authentication key for distribution to the SG, as described above.

8.2 Authentication credentials

Unlike the number of endpoints, the number of SGs in a multi-region network is expected to be relatively small. In most cases, it is expected that service will be provided by subscription, or other contractual agreement, hence the gatekeeper will be provisioned with some identifying information about the SGs which might register with it. In the simplest case, SGs could be assigned passwords, and H.235.1, H.235.2, H.235.3, H.235.5 or challenge-response authentication procedures could be employed. The use of pre-shared secrets requires a secure out-of-band mechanism for their distribution, of course.

An alternative mechanism might be based on public key certificates. Copies of the gatekeeper's certificate (or of the certificate belonging to the authority which signed the gatekeeper's certificate) could be installed to the SGs through some trusted process. The use of certificate methods remains for further study.

9 Security considerations

Protocols of this type, in which a message is permitted to be modified in transit, are subject to downgrade attacks. For example, if an endpoint offers both encrypted and unencrypted media transport capabilities, a malicious SG could remove the encryption offers and simply supply the unencrypted ones, thereby insuring that the media streams would be unencrypted. This type of attack must be countered by the endpoints (and the gatekeeper) by offering only those capabilities that are acceptable according to their own security policy. Ultimately, it is the responsibility of the endpoints and their users to insure that the appropriate security level is established and maintained. Similar considerations apply to the choice of security profiles during registration: if an endpoint requires strong authentication, it should specify so in its GRQ, and it should not accept a weaker offer from a gatekeeper.

10 Applicability

This scheme will be applicable to other H.235.1, H.235.2 and H.235.3 security profiles in addition to those described in ITU-T Rec. H.235.5. Any security profile which provides for the negotiation/derivation of suitable authentication keys may be supported. The SGs should examine elements of the GRQ/GCF (e.g., **authenticationCapability** and/or **authenticationMode**) to see if they can support the negotiated message authentication or security scheme.

11 Object Identifier

OID	Object identifier value	Description
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	ClearToken carrying profile elements for SG discovery.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006