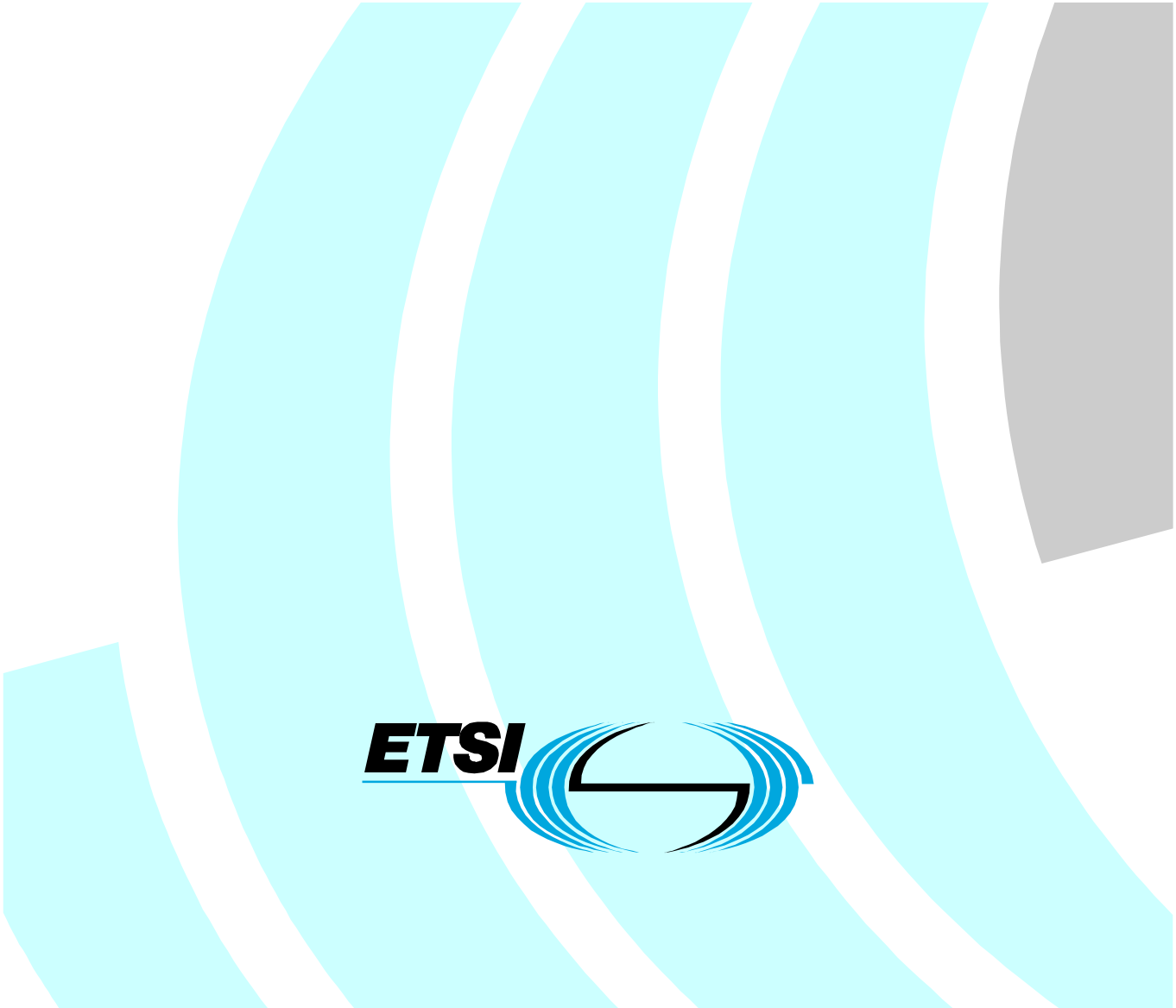
ETSI TS 102 466 V1.1.1 (2007-01)

Technical Specification

Satellite Earth Stations and Systems (SES);
Broadband Satellite Multimedia (BSM);
Multicast Security Architecture



Reference
DTS/SES-00106

Keywords
broadband, interworking, IP, satellite, security,

ETSI

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

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

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

Contents

Intellectual Property Rights 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 BSM Secure Multicast Service Requirements 8
4.1 Multicast threat analysis 8
4.2 Multicast service scenarios 9
4.2.1 Scenario 1: End-to-end secure multicast - External multicast source to BSM 9
4.2.2 Scenario 2: Multicast group with static membership 10
4.2.3 Scenario 3: Multicast group with dynamic membership 10
4.2.4 Scenario 4: Multiple senders 11
4.2.5 Scenario 5: Composite group key management between BSM and non-BSM domains 11
4.3 Summary of multicast security service requirements 12
5 BSM Multicast Security Functional Architecture Requirements 12
5.1 Multicast security reference framework 13
5.1.1 Multicast data handling (privacy and integrity) 14
5.1.2 Group Security Association (GSA) 14
5.1.2.1 Registration Security Association 15
5.1.2.2 Rekey Security Association 15
5.1.2.3 Data Security Association 16
5.1.3 Key management 16
5.1.3.1 Registration Protocol 16
5.1.3.2 Rekey Protocol 17
5.1.3.3 Data Security Protocol 17
5.1.4 Security policy establishment and enforcement 18
5.1.5 Example multicast key management systems 19
5.2 Generic BSM multicast architecture 19
5.3 Interactions between security and other non BSM entities 20
5.3.1 Interactions with AAA 20
5.3.2 Interactions with COPS 20
5.3.3 Interactions between BSM security and Network Address Translation (NAT) 20
5.3.4 Interactions with IPv6 related entities 21
5.4 Summary of multicast key management requirements 21
6 BSM Multicast Security Functional Architecture Definition 22
6.1 Detailed BSM security functional architecture 22
6.1.1 Case 1: Secure multicast in the Satellite Dependent (SD) layer (below SI-SAP) 23
6.1.2 Case 2: Secure multicast with network layer security (above SI-SAP) 24
6.1.3 Case 3: Mixed secure multicast (security manager above SI-SAP and security engine below SI-SAP) 25
6.1.4 Case 4: End-to-end secure multicast 26
6.1.5 Case 5: Secure multicast in composite groups (BSM and non-BSM membership) 27
6.2 Interactions between multicast security and QoS BSM entities 27
6.2.1 QoS provisioning for key management messages 27
6.2.2 Securing RSVP and Diffserv message exchanges 28
6.3 Interactions between multicast security and multicast source management entities 30
Annex A (informative): The current DVB-RCS security system 31
A.1 DVB-RCS Authentication 31

A.2 Transport of security messages 32
A.3 DVB-RCS multicast extensions 33

Annex B (informative): IPSec extensions for multicast 35

B.1 Security Association Modes 35
B.1.1 Tunnel Mode with Address Preservation 35
B.2 Modifications to IPsec Databases 36
B.3 Data Origin Authentication 36
B.4 Interworking between unicast and multicast Key Management 37
B.5 IPv4 NAT issues 37
B.6 Avoidance of NAT Using an IPv6 Over IPv4 Network 38

Annex D (informative): Bibliography 39

History 40

Intellectual Property Rights

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

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 ETSI 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 Technical Committee Satellite Earth Stations and Systems (SES).

Introduction

The aim here is to build an open specification for secure IP multicast service delivery via satellites. The present document are be based on current ETSI BSM architecture documents. Also it is aligned with the relevant IETF standards such as IPsec, MSEC and IP-over-DVB recommendations (RFCs).

1 Scope

The present document provides a multicast security architecture for secure multicast services over BSM networks, maintaining interworking with the Internet architecture. It specifies the multicast security reference framework and the security services that can be part of a secure multicast solution. Its focus is on functional areas such as multicast group key management and data handling.

The following topics are out of scope for the present document:

- Detailed definition, construction and modification of multicast security policies.
- Securing multicast management and control messages for On Board Processing (OBP) satellites.
- Security for reliable multicast (such as Internet RMT work) is out of scope as well.

This work builds on the earlier work in the general security architecture TS 102 465 [1] and the Security Aspects report (BSM TR 102 287 (see bibliography)).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI TS 102 465: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); General Security Architecture".

[2] ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".

[3] ETSI TS 102 463: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with IntServ QoS".

[4] ETSI TS 102 294: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; IP interworking via satellite; Multicast functional architecture".

[5] ETSI TS 102 464: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Interworking with DiffServ Qos".

[6] ETSI TS 102 461: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multicast Source Management".

[7] ETSI TS 102 462: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); QoS Functional Architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 465 [1] apply.

3.2 Abbreviations

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

AH	Authentication Header
ATM	Asynchronous Transfer Mode
CGD	Composite Group Distributor
COPS	Common Open Policy Service
DCKS	Domain Controller and Key Server
DES	Data Encryption Standard
DoS	Denial of Service
DVB	Digital Video Broadcast
DVB-RCS	DVB-Return Channel Satellites
DVB-S	Digital Video Broadcast by Satellite
EKE	Explicit Key Exchange
ESP	Encapsulated Security Payload
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
GC	Group Controller
GCKS	Group Controller Key Server
GKMP	Group Key Management Protocol
GS	Guaranteed Service
GSA	Group Security Association
GSPD	Group Security Policy Database
HMAC	Hash based Message Authentication Code
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
ITU	International Telecommunication Union
LKH	Logical Key Hierarchy
MAC	Message Authentication Code
MKE	Main Key Exchange
MPE	Multi Protocol Encapsulation
MPEG	Moving Picture Experts Group
MPEG-TS	MPEG Transport Stream
MSEC	Multicast SECurity group in the IETF
NAT	Network Address Translation
NCC	Network Control Centre
OBP	On Board Processing
PEP	Performance Enhancing Proxy
PID	Packet IDentifier
PKI	Public Key Infrastructure
PDP	Policy Decision Point
PEP	Policy Enforcement Point
QKE	Quick Key Exchange
QoS	Quality of Service
RCST	Return Channel Satellite Terminal
RMTP	Reliable Multicast Transport Protocol
RSA	Rivest, Shamir and Adleman
RTCP	Real time Transport Control Protocol
RTP	Real time Transport Protocol
SA	Security Association
SDAF	Satellite Dependent Adaptation Function

SIAF	Satellite Independent Adaptation Function
SID	Security association IDentity
SIP	Session Initiation Protocol
SI-SAP	Satellite Independent Service Access Point
SPI	Security Parameter Index
SSM	Source-Specific Multicast
ST	Satellite Terminal
TEK	Traffic Encryption Key
ULE	Unidirectional Lightweight Encapsulation
VPN	Virtual Private Network

4 BSM Secure Multicast Service Requirements

4.1 Multicast threat analysis

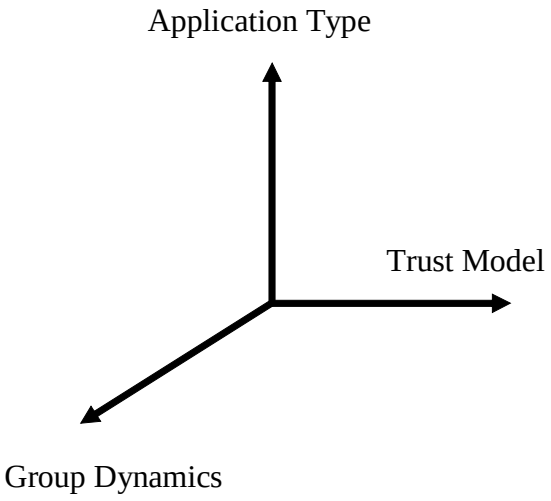


Figure 1: Factors affecting secure multicast system design

There are several interrelated factors or aspects of IP Multicast that influence the approaches and mechanisms used to secure it (details are presented in TR 102 287 (see bibliography)) and shown in Figure 1. The most relevant factors include:

- Multicast application type.
- Group dynamics and Scalability issues.
- Underlying trust model.

The secure BSM multicast groups can be large and dynamic. Therefore multicast key management is considered the most complex issue that need to be addressed in details.

The general security architecture TS 102 465 [1]and the security aspect report TR 102 287 (see bibliography) documents have analysed the security threats to BSM networks and services. They also provides the counter measures needed against such threats. The same threat analysis and counter measures are applicable to the present document. For example, threats and potential attacks on the BSM entities are categorized into 4 types: Network, software, hardware and human threats. The network threats are the major focus of the present document.

In addition, there is further analysis of threats to IP transmission over DVB networks in draft-cruickshank-ipdvb-sec-req-04.txt (see bibliography). For the purpose of the present document, three threat examples have been identified:

EXAMPLE 1: Monitoring: The intruder monitors (passively) the satellite broadcasts in order to gain information about data and/or tracking the communicating parties.

EXAMPLE 2: Local high jacking of the satellite transmission: Here it is assumed that the intruder is sophisticated and able to block the original transmission from the satellite system and deliver a modified version of the MPEG-TS transmission to a single satellite Receiver or a small group of Receivers (e.g. in a single company site). The global satellite system might not be aware of such attacks.

EXAMPLE 3: Global high jacking of the satellite transmission: Again it is assumed that the intruder is very sophisticated and able to high jack the whole satellite transmission to all Receivers.

The above analysis shows the need for BSM security services such as data confidentiality, integrity, sender authentication/authorization and efficient key management system. These security services are defined in TS 102 465 [1], clause 4.2.

4.2 Multicast service scenarios

This clause presents some high level scenarios that highlight key management issue for secure multicast services in BSM networks. Each scenario should counter all of the threats identified above.

Security policies play an important role in defining the rules that govern a secure multicast session and the privileges of each ingress ST/Gateway (multicast sender) and egress STs (multicast receiver). All BSM security entities will enforce the rules of these policies.

4.2.1 Scenario 1: End-to-end secure multicast - External multicast source to BSM

This scenario is transparent to BSM. The BSM network plays no part in the secure multicast service setup or management. The multicast source (IP host/server), receivers (IP host) and key management are outside the BSM security administrative domain. Figure 2 shows this scenario, where the access to BSM network is controlled and managed by the BSM multicast source management functions (described in TS 102 461 [6]).

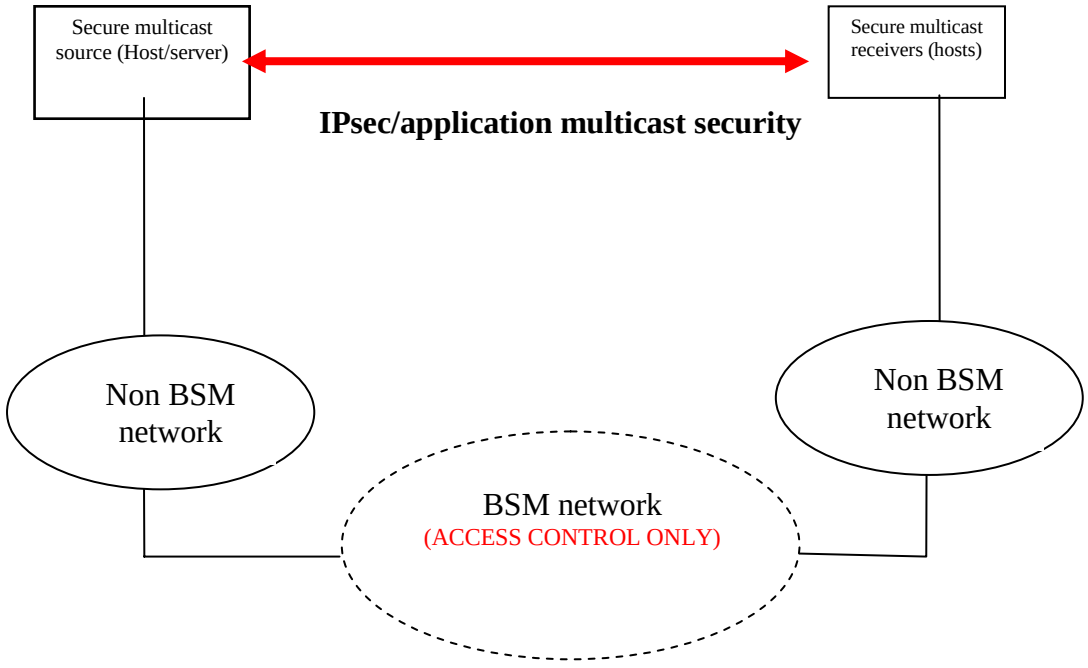


Figure 2: Scenario 1: End-to-end multicast group - BSM transparent

4.2.2 Scenario 2: Multicast group with static membership

This scenario covers the BSM secure multicast services, where the group membership is fixed. In other words, the BSM security manager has a fixed list of ingress/egress STs. The egress STs may join the secure session before or during the multicast session. One practical example of such scenario is a Virtual Private Network (VPN) over BSM network.

The key management procedures here are simple: Initially, the secure multicast group members shall be authenticated by the BSM key management server. The data encryption key and key management messages (generated by the BSM key management server) are distributed to all ingress and egress STs (by unicast or multicast transmissions). These keys can either be fixed for the whole duration of multicast session, or updated periodically (depending on the group policy). Figure 3 shows this scenario, where the security policy defines the rules for the secure group and the data security is the actual encryption/integrity of the multicast data.

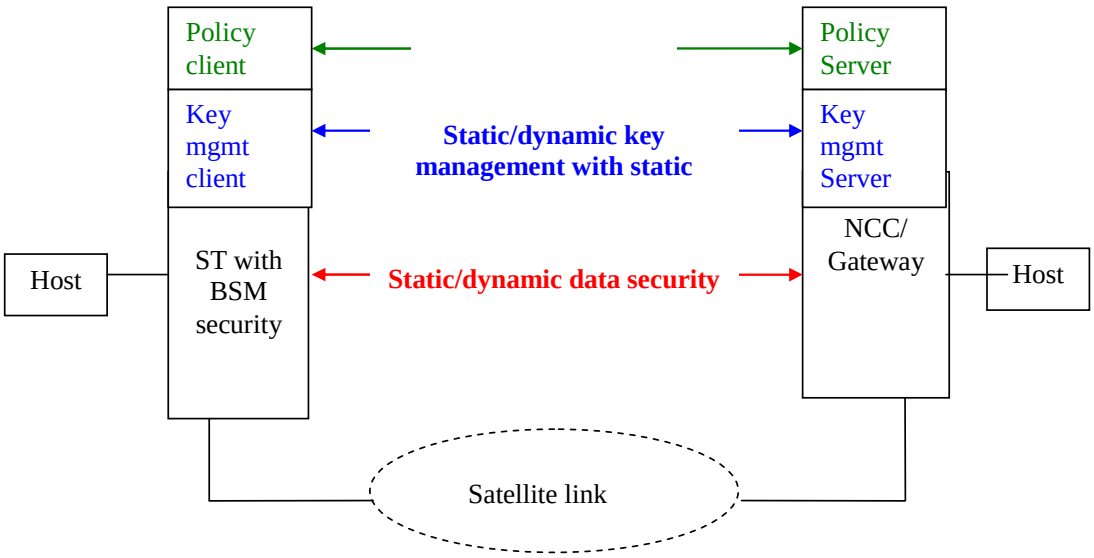


Figure 3: Static multicast key management

4.2.3 Scenario 3: Multicast group with dynamic membership

This scenario covers the BSM secure multicast services, where the secure multicast group membership can vary with time (Figure 4), assuming that there is a single ingress ST/gateway, The number of egress STs in a secure multicast session is dynamic. In other words, the BSM key management server has to manage a variable number egress STs. One example of such scenario an Internet Service Provider (ISP) providing a real time streaming service to a group of customers.

The key management procedures are more complex than scenario 2: The BSM key management server may perform the following tasks:

- Authentication of the secure multicast group members.
- Distribute keys to STs that are members of this session at the time of their joining the group.
- Re-key when an ST joins and/or leaves (depending on the rules in the security policy for this group).
- Periodic rekeying if required.

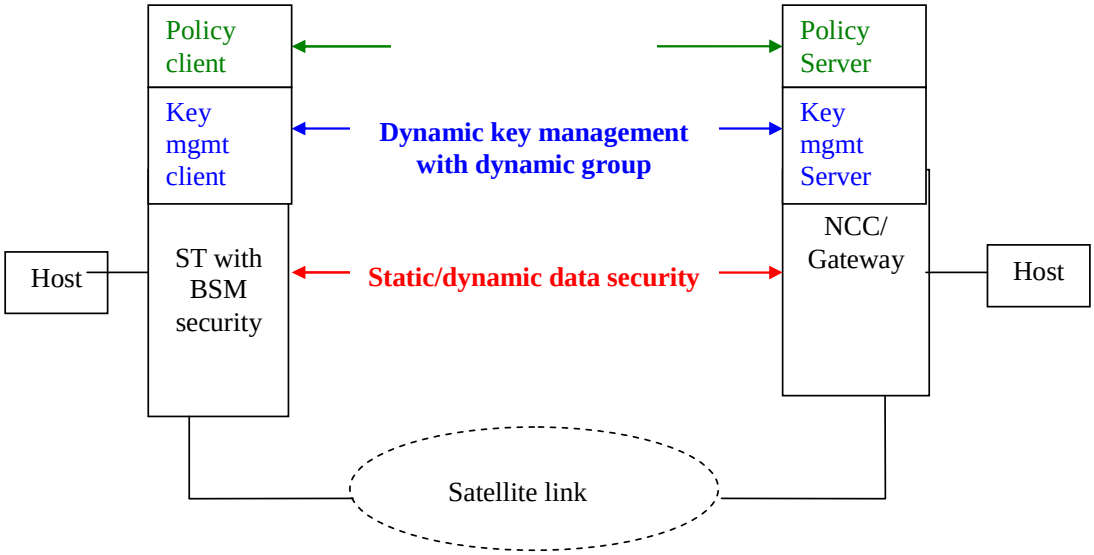


Figure 4: Dynamic multicast key management

4.2.4 Scenario 4: Multiple senders

The group management here can be either dynamic or static. However let us assume it is a dynamic group. One example of such scenario is a multimedia conferencing over BSM with multiple ingress STs.

Similar to scenario 3 (Figure 4), the BSM key management server has to perform key distribution and re-keying tasks. In addition, there can be two types of security association for ingress STs:

- Scenario 4a: All ingress STs share one key and one security association.
- Scenario 4b: Each ingress ST has its own key and security association.

Scenario 4a is the simpler of the two, where one key and one security association is used for the whole group (all ingress and egress STs). However, protection against replay attacks is not possible because sequence numbering of secure packets is not possible in the presence of multiple senders (ingress STs).

For scenario 4b, each egress ST needs to handle multiple decryption keys in a multicast session (one key per ingress ST). Protection against replay attacks is possible with the use of one sequence number set per ingress ST.

In general, multiple source groups have special requirements for protection against Denial of Service (DoS) and for minimizing state needed for sender authentication. There can be two access control levels: The BSM **Local** and **Network** security managers to allow or deny ingress STs sending to the group. Therefore strict sender rules and a well defined security policies are critical to prevent DoS attacks.

4.2.5 Scenario 5: Composite group key management between BSM and non-BSM domains

Figure 5 shows a composite group made up of three subgroups with a centralized key management based on the BSM key management server. Such scenario is useful for large scale multicast groups with many multicast receivers but only few speakers. An example of this scenario is a multicast group that spans several security domains such as BSM, UMTS and terrestrial Internet, which requires using different keys for each domain due to operational or policy reasons.

In this scenario, we assume that subgroup 1 is in the BSM security domain. Subgroups 2 and 3 are located in non-BSM security domains, which might have different cryptographic requirements than the BSM domain (such as using encryption keys with different lengths). The key management and the composite domain distributor for such a group are described further in annex C and clause 6.1.5.

The key management can be either static or dynamic for the composite group as described in scenario 2 or 3 (clauses 4.2.2 and 4.2.3 respectively). Therefore BSM Domain (domain 1) features are not shown in Figure 5.

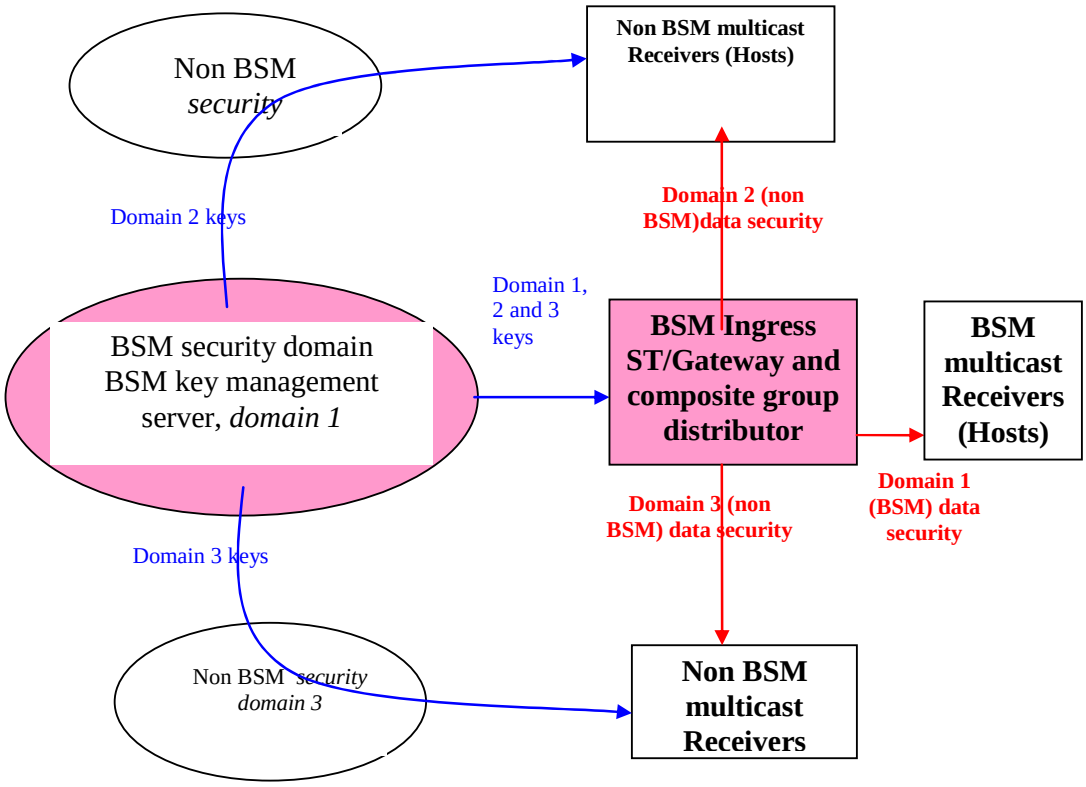


Figure 5: Multicasting across heterogeneous security domains

4.3 Summary of multicast security service requirements

The threat analysis and scenarios presented in clauses 4.1 and 4.2 show the need for the following security requirements:

- Security key management shall be scalable in order to cater for large and dynamic multicast groups.
- Data confidentiality is the major requirement against passive threats to satellite links.
- In a multiple senders scenario (such as conferencing), strict control is required for all ingress STs in a multicast session, in order to prevent Denial of Service attacks.
- Decoupling of BSM multicast key management functions from BSM data encryption. This will allow the re-use of existing security management systems (e.g. GDOI RFC 3547 and GSAKMP RFC 4535 [11], plus other systems such as DVB-RCS (see EN 301 790) and/or the development of new systems, as required.
- For end-to-end secure multicast, BSM role is confined only to access control to the BSM resources.
- Optional security for QoS and other management control messages (e.g. bandwidth requests).

Further analysis of the multicast key management requirements are presented in clause 5.3.

5 BSM Multicast Security Functional Architecture Requirements

This clause describes the BSM multicast security architecture building blocks (reference framework) and interactions with non-BSM entities such as COPS, AAA, and IPv6 related functional entities.

5.1 Multicast security reference framework

This work is based BSM general security architecture in TS 102 465 [1] and focused on multicast functional and key management issues.

In the present document, Figure 6, shows the Reference Framework is based on three broad functional areas. These functional areas were described in TS 102 465 [1], in clause 5.1, Figures 6 and 7.

In the present document, Figure 6, shows the main entities and functions relating to multicast security, and depicts the inter-relations among them. It also expresses the complex multicast security from the perspective of architecture (centralized and distributed), multicast group types (1-to-*N* and *M*-to-*N*), and classes of protocols (the exchanged messages) needed to secure multicast packets.

Regarding the scenarios presented in clause 4, a single sender corresponds to 1-to-N type and multiple senders corresponds to M-to-N type. The BSM **Network** security manager correspond to the Domain Controller and Key Server (DCKS) in Figure 6. The sender and receivers can be interpreted as end server/hosts or BSM ingress/egress STs. They show the place where encryption/decryption is applied.

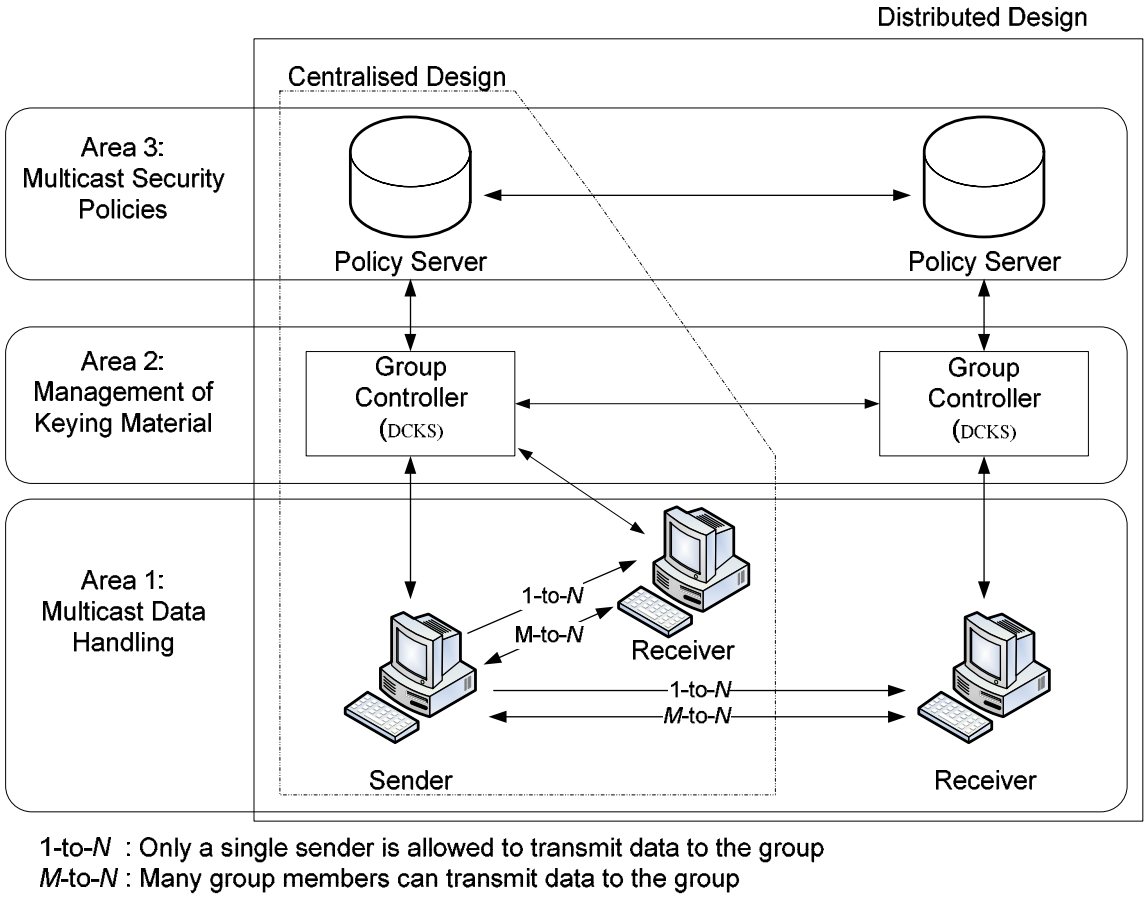


Figure 6: Secure multicast reference framework

The Reference Framework can be viewed horizontally and vertically. Horizontally, it displays both the entities and functions as singular boxes, expressing each of the three broad problem areas (i.e. multicast security policies, management of keying material and multicast data handling). Vertically, it expresses the basic architecture designs for solutions; namely, a centralized architecture and a distributed architecture. In short, a distributed design is a superset of the centralized design which involves more than one group controllers and policy servers. This helps to prevent a single point of failure and performance bottleneck in the centralized design. In clause 4, all scenarios presented multicast services in a centralized architecture.

Distributed key management is out of scope in the present document, although scenario 5 can be adapted for distributed key management architecture between BSM and non-BSM domains. However, there is a strong link between distributed key management and using security policies.

5.1.1 Multicast data handling (privacy and integrity)

This corresponds to functional area 1 in Figure 6. In a secure multicast group, the multicast data typically need to be:

- Encrypted using a group key, mainly for access control or confidentiality.
- Join authentication: New members shall be authenticated using the registration protocol specified in clause 5.1.3.1.
- Authenticated, for verifying the source and integrity of the data. Authentication takes two flavours:
  - *Source authentication:* This functionality guarantees that the multicast data originated by the claimed source and was not modified en route (either by a group member or an external attacker). Typically, examples of source authentication algorithms are: TESLA RFC 4082 or RSA digital signature RFC 4359 (see bibliography).
  - *Group authentication*: This type of authentication only guarantees that the data generated (or last modified) by some group members. It does not guarantee data integrity unless all group members are trusted. Typically, Message Authentication Code (MAC) is used to provide group authentication.

For data secrecy, the sender needs to encrypt the data stream with a secret key which is known by all group members that are authorized to receive multicast data stream. When the group becomes large, scalable distribution and rekeying of a group key can be a complex problem. TR 102 287 (see bibliography) presents the a scalable solution for keying to large multicast groups. The solution called Logical Key Hierarchy (see clause 8.4.1 in TR 102 287 (see bibliography) for details).

5.1.2 Group Security Association (GSA)

This also corresponds to functional area 1 in Figure 6. In the context of unicast, the two-party Security Association (SA) management model is used to secure the communication between both parties. For example an SA in the Internet Protocol Security (IPSec) is identified by a Security Parameter Index (SPI). However, the unicast SA is simply not mapable to groups in the case of IP multicast, and the wider field of group communications, as there are many group members (senders and receivers). A GSA contains all of the SA attributes in point-to-point key management (i.e. attributes include cryptographic keys, algorithm, identifier and other related attributes used to associate with the security material), as well as some additional attributes pertaining to the group.

The GSA is an aggregate of three categories of SAs. The first one is a "pull" SA between the group member and the DCKS, second is a "push" SA between the DCKS and all the group members, and the third is an SA to protect application data from the sender-members to receiver-members. In fact, each sender to the group may use a unique key for their data and use a separate SA. These three categories of SAs, which correspond to three different kinds of communications commonly required for group communications, are shown in Figure 7. These categories are elaborated further in the following clauses.

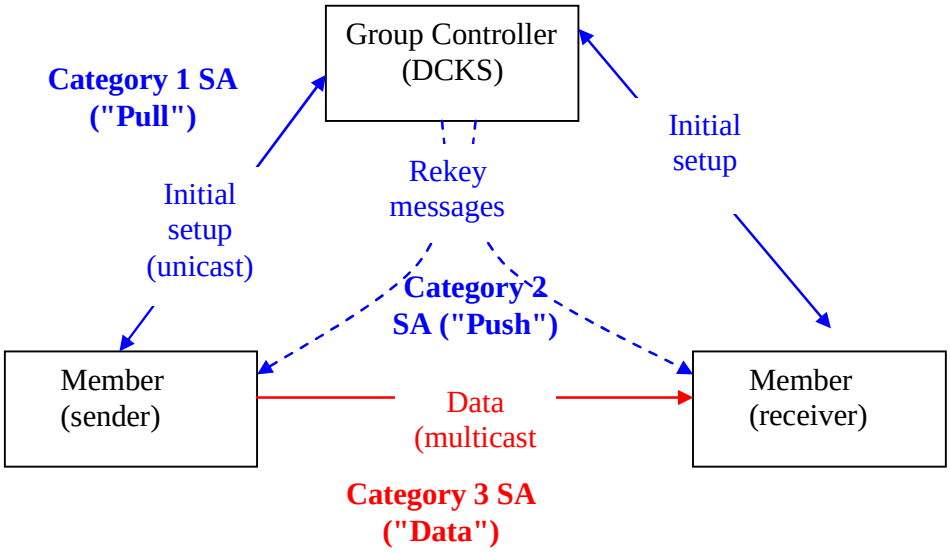


Figure 7: Group Security Association (GSA) definition

5.1.2.1 Registration Security Association

This is sometime called Category 1 SA (pull SA between the group member and the DCKS). This SA is required for (bi-directional) unicast communications between the DCKS and a group member (be it a sender or receiver). The DCKS entity is charged with access control to the group keys, with policy distribution to members (or prospective members), and with group key dissemination to member-sender and member-receiver.

This Registration SA is initiated by the member to pull the GSA information from the DCKS. This is how the member requests to join the secure group, or has its GSA keys re-initialized after being disconnected from the group. The GSA information pulled down from the DCKS includes the SA, keys and policy used to secure the data transmission between sending and receiving members. This SA is used to protect the other elements of the GSA (such as the other following two categories of SAs), either in a "push" or "pull" model.

However, the requirement of a registration SA does not imply the need of a registration protocol to create that Registration SA. The Registration SA could instead be setup through some manual means, such as distributed on a smart card. Thus, what is important is that a Registration SA exists, and is used to protect the other SAs.

5.1.2.2 Rekey Security Association

Sometimes this is called Category 2 SA (push SA between the DCKS and all the group members). An SA is required for the multicast transmission of rekey messages (unidirectional) from the DCKS to all group members. As such, this SA is known by the DCKS and all members of the group. Rekey messages may result from group membership changes, from changes in group security policy, from the creation of new traffic-protection keys for the particular group, or from key expiry. The DCKS shall ensure that all members receive the rekey information in a timely manner. In addition, the member should contact and resynchronize with the DCKS if their keys expired or an updated key has not been received.

This SA is not negotiated, since all the group members shall share it. Thus, the DCKS shall be authentic source and act as the sole point of contact for the group members to obtain this SA. In some cases, this rekey SA is not absolutely required to be part of a GSA. For example, the lifetime of some groups may be short enough such that a rekey is not necessary.

5.1.2.3 Data Security Association

This is sometimes called Category 3 SA (SA to protect data from the sender-members to receiver-members). One or more SAs are required for the multicast transmission of data messages (unidirectional) from the sender to other group members. This SA is known by the DCKS and by all members of the group. Similarly, regardless of the number of instances of this third category of SA, this SA is not negotiated. Rather, all group members obtain it from the DCKS. The DCKS itself does not use this category of SA. If the group has more than one Data Security SA, the data security protocol shall have a means of differentiating the SAs (e.g. with a SPI). There are a number of possibilities with respect to the number of the Data Security SAs:

i) Each member-sender in the group could be assigned a unique Data Security SA, thereby resulting in each member-receiver having to maintain as many Data Security SAs as there are member-senders in the group. In this case, each source may be verified using source origin authentication techniques.

ii) The entire group deploys a single Data Security SA for all member-senders. Member-receiver would then be able to maintain only one data security SA.

iii) A combination of 1 and 2.

The use of a single Data Security SA for all member-senders or a Data Security SA for each member-senders was illustrated in the scenario 4 in clause 4.2.4 (multiple senders scenario).

5.1.3 Key management

This also corresponds to functional area 2 in Figure 6. It is concerned with the security of distribution and refreshment of keying material. The term "keying material" refers to the cryptographic key belonging to a multicast group, the state associated with the keys and the other security parameters related to the keys.

Clause 6.2.2 show a method to increase the reliability of exchanging "keying material" by using the QoS provisioning features in BSM.

A group key management protocol supports protected communication between members of a secure group. As group membership may vary over time, a group key management protocol shall ensure that only members of a secure group can gain access to group data (by gaining access to group keys) and authenticate group data. The goal of a group key management protocol is to provide legitimate group members with the up-to-date cryptographic state they need for secrecy and authentication. See clause 4 for static and dynamic group scenarios.

The main goal of a group key management protocol is to securely provide group members with an up-to-date SA, which contains the needed information for securing group communication (i.e. the group data). This SA is known as the Data SA. In order to achieve this goal, the MSEC group key management architecture defines the following protocols, which follows the SA categories presented in clause 5.1.2.

5.1.3.1 Registration Protocol

In this protocol, the GC and a joining member mutually authenticate each other. If the authentication succeeds and the GC finds that the joining member is authorized, then the GC supplies the joining member with the following information:

- Sufficient information to initialize the Data SA within the joining member. This information is given only if the group security policy calls for initializing the Data SA at registration.

- Sufficient information to initialize a Rekey SA within the joining member. This information is given if the group security policy calls for a rekey protocol.

Some registration protocols need to tunnel through a data-signalling protocol to take advantage of existing security functionality, and/or to optimize the total session setup time. It may be advantageous to tunnel the key exchange procedure inside call establishment (MIKEY RFC 2830 (see bibliography)) so that both can complete at the same time.

The registration protocol shall ensure that the transfer of information from GC to member is done in an authenticated and confidential manner over a registration SA. A complementary de-registration protocol serves to explicitly remove Registration SA state.

5.1.3.2 Rekey Protocol

The purpose of the group rekey protocol is for transport of keys and SAs between a GC and the members of a secure group. The GC may periodically update or change the Data SA, by sending rekey information to the group members. Rekey messages may result from group membership changes from:

- Changes in group security policy.
- Creation of new traffic keys or key distribution keys.
- Key expiry.

Generally, the goals of the rekey protocol are:

- To synchronize a GSA.
- To provide privacy and (symmetric and asymmetric) authentication, replay protection and DoS protection.
- Efficient rekeying after changes in group membership or when keys expire.
- Reliable delivery of rekey messages.
- Member recovery from an out-of-sync GSA.
- Support multicast or multi-unicast.

Rekey messages are protected by the Rekey SA, which is initialized in the registration protocol. They contain information for updating the Rekey SA and/or the Data SA and can be sent via multicast to the group members or via unicast from the GC to a particular group member. There are two methods of authenticating rekey messages:

- group-based and;
- source authentication.

The rekey protocol ensures that all members receive the rekey information in a timely manner. In addition, the rekey protocol specifies mechanisms for the parties to contact the GC and re-synch if their keys expired and an updated key has not been received. The rekey protocol for large-scale groups offers mechanism to avoid implosion problems and to ensure reliability in its delivery of keying material. TR 102 287 (clause 8.4.1) presents the a scalable solution for keying to large multicast groups called Logical Key Hierarchy (LKH).

Although the Rekey SA is established by the registration protocol, it is updated using a rekey protocol. When a member departs the group, it destroys its local copy of the GSA. Using a de-registration message may be an efficient way for a member to inform the GC that it has destroyed, or is about to destroy, the SAs. Such a message may prompt the GC to cryptographically remove the member from the group (i.e. to prevent the member from having access to future group communication). In large-scale multicast applications, however, de-registration can potentially cause implosion at the GC.

5.1.3.3 Data Security Protocol

The data security protocol uses Traffic Encryption Keys (TEKs) to protect data streams sent and received by the data security protocol. Thus the registration protocol and/or the rekey protocol establish the Key Encryption Keys (KEKs) and TEKs. Regardless of the data security protocol used, the GC is responsible for supplying the TEKs, or information to derive the TEKs for traffic protection.

Figure 8 depicts the design of a group key management protocol. Each group member, sender or receiver, uses the registration protocol to get authorized and authenticated access to a particular group, its policies, and its keys. The two types of key used are the KEKs and TEKs. For group authentication of rekey or data, key integrity or traffic integrity keys may be used, as well. The KEK may be a single key that protect the rekey message, typically containing a new Rekey SA (containing a KEK) and/or Data SA (containing a TEK).

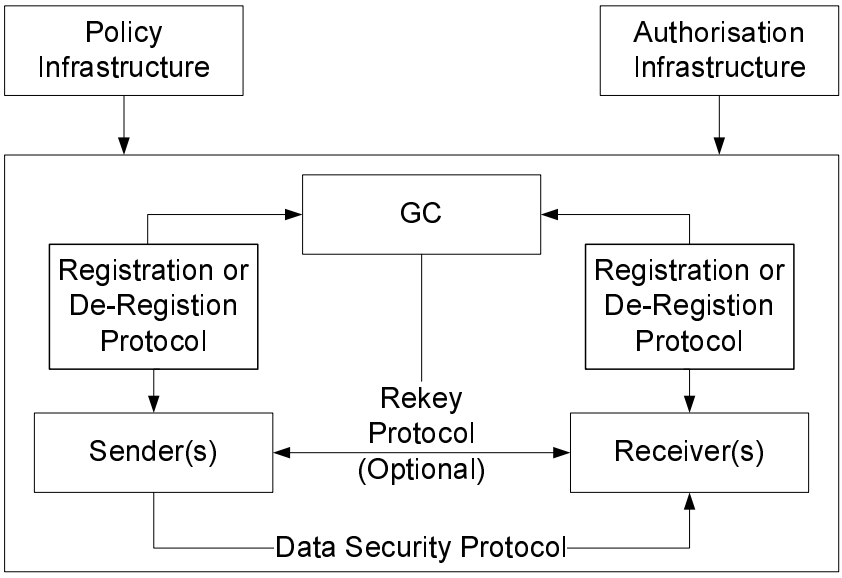


Figure 8: Design of a group key management model

There are a few distinct outcomes to a successful registration protocol exchange:

- If the GC uses rekey messages, then the admitted member receives the Rekey SA. The Rekey SA contains the group's rekey policy, and at least one group KEK. In addition, the GC sends a group integrity key for integrity protection of rekey messages. If a group key management algorithm is used for efficient rekeying, the GC also sends one or more KEKs as specified by the key distribution policy of the group key management.

- If rekey messages are not used for the group, then the admitted member receives TEKs (as part of the Data Security SAs) that are passed to the member's data security protocol.

- The GC may pass the KEKs or TEKs to the member even if rekey messages are used, for efficiency reasons and according to group policy.

It is also important to note that the rekey protocol is primarily responsible for scalability of the group key management architecture. Hence, it is imperative that the above listed properties are provided in a scalable manner. For instance, the rekey properties may use a scalable group key management algorithm to reduce the number of keys sent in a rekey message.

5.1.4 Security policy establishment and enforcement

The general framework for using security policies is described in TS 102 465 [1]. BSM Security Policies shall provide the rules for operation for all the elements of the multicast reference framework.

Security policy design and detailed description is out of scope of the present document. the communication protocols between the Policy Server and the Key Server can be realized using various mechanisms:

- Using standard policy infrastructure such as a COPS Policy Decision Point (PDP) and Policy Enforcement Point architecture (PEP) (RFC 2748 and RFC 3084 (see bibliography)).

- Using the key management protocol to transfer the security policy such as the GSAKMP protocol (see clause 5.1.5 for more details).

- Using other protocols such as Session Initiation Protocol (SIP) to transfer the security policy or even through web services.

At minimum, however, this security service will be realized in a set of policy definitions, such as every session security conditions and actions.

5.1.5 Example multicast key management systems

The BSM report on Security Aspects (BSM TR 102 287, clause 8.4.2 (see bibliography)) has existing several examples of multicast key management systems such as GSAKMP, GDOI, MIKEY and KMKE. These key management systems can be implemented in BSM networks in conjunction with link or network layer security.

5.2 Generic BSM multicast architecture

Figure 9 presents the BSM protocol stack specific to multicast; it is taken from the BSM multicast functional architecture document (TS 102 294 [4]). Figure 9 shows how the basic set of functions and SI-SAP primitives for unicast Internet connectivity is complemented by multicast specific functions.

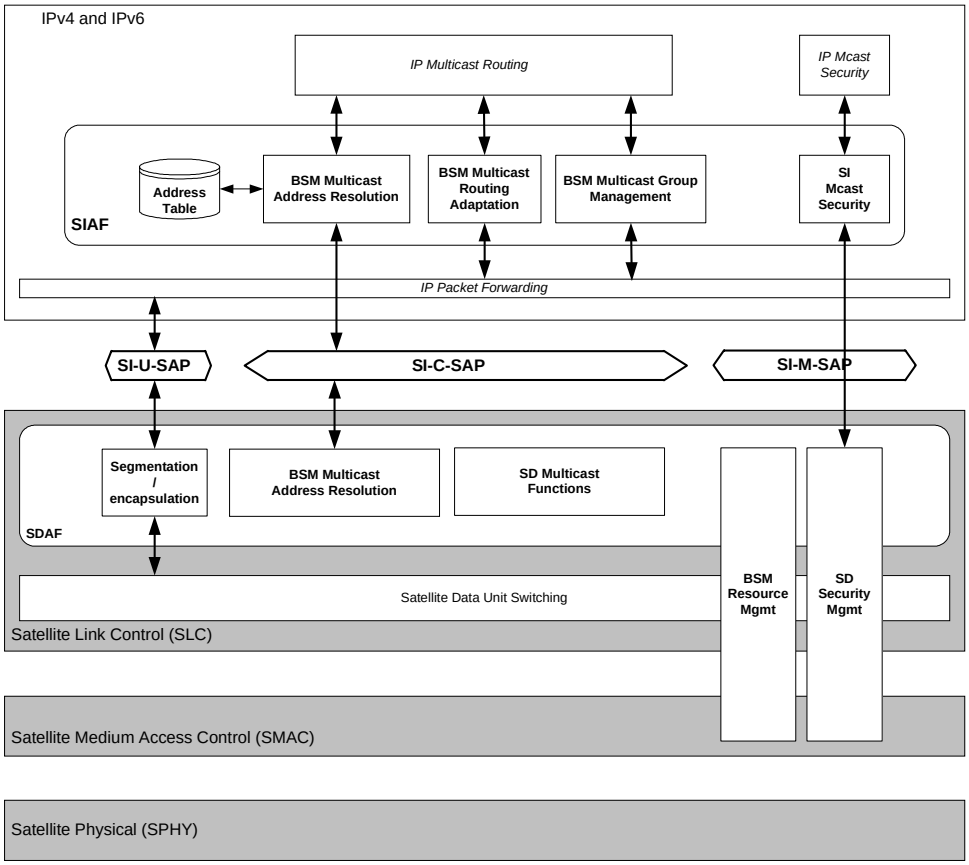


Figure 9: OSI protocol stack for BSM multicast services

The security reference framework presented in clause 5.1 (with the related key management protocols and policy distribution) fits into this generic BSM multicast architecture (Figure 9). The detailed security interactions across the SI-SAP are presented in clause 6.1.

Figure 10 shows the timing sequence for multicast security message exchanges between the security client (ST) and the security server (NCC/Gateway). It shows the key exchange protocols (registration, secure data and rekeying) described in clause 5.1.3. Figure 10 is shows the position of security exchanges in relation to the multicast source management signalling (TS 102 461 [6]).

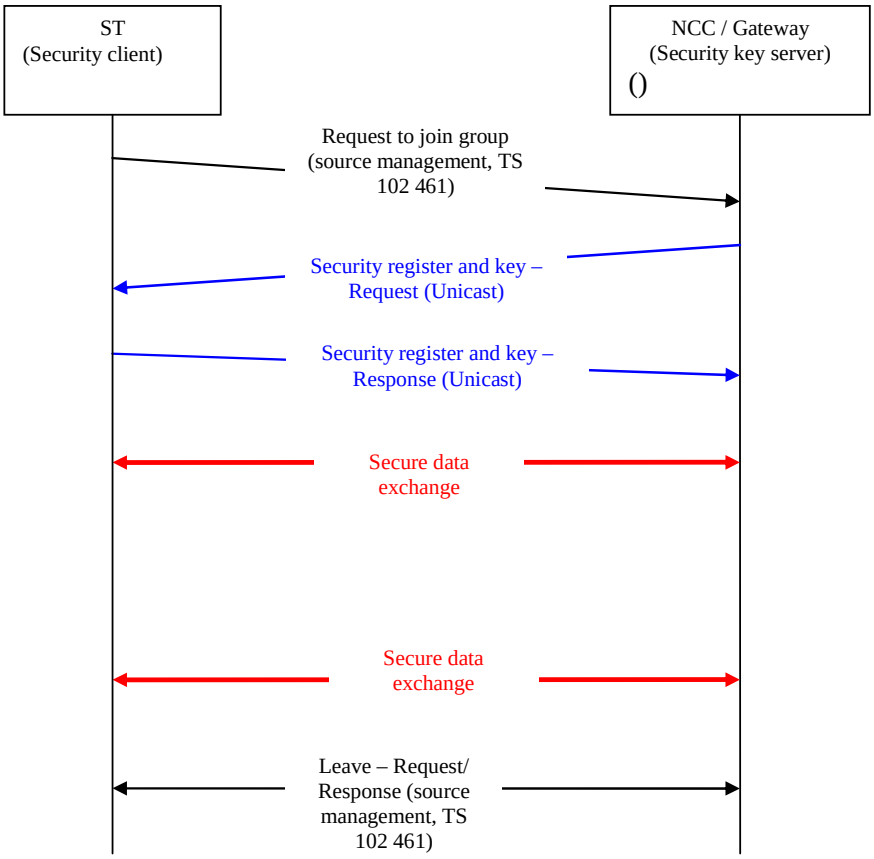


Figure 10: Sequence diagram for multicast key management messages exchanges

5.3 Interactions between security and other non BSM entities

5.3.1 Interactions with AAA

The security architecture TS 102 465 [1], clause 5.3.2, recommendation apply here for secure multicast over BSM networks.

5.3.2 Interactions with COPS

The security architecture TS 102 465 [1], clause 5.3.1, recommendation apply here for secure multicast over BSM networks.

5.3.3 Interactions between BSM security and Network Address Translation (NAT)

In general the use of NATs should be avoided in BSM networks, which has impact on the security system implementation with IPsec. However, if NAT is used, then the security architecture TS 102 465 [1],clause 5.3.3, had addressed this issue and its recommendation is to use UDP encapsulation of IPSec ESP packets as specified in RFC 3948 and IPSec key management and NAT traversal as specified in RFC 3947 (see bibliography).

For secure multicast the same recommendation will apply, taking into account the modifications needed for IPsec as presented in annex B. However, this capability shall be configured at the GCKS as a group policy, and it shall be supported in unison by all of the multicast group endpoints (such as BSM STs in scenarios 2, 3 and 4 in clause 4; and cases 2 and 5 in clause 6).

NAT issues are transparent to BSM networks if security implemented in the link layer such DVB-RCS security system (such as cases 1 and 3 in clause 6).

5.3.4 Interactions with IPv6 related entities

In an all IPv6 BSM network, secure multicast issues are similar to an all IPv4 BSM network. However, if IPv6 and IPv4 combinations are used, then additional security issues related to the use of NATs (as described in clause 5.2.3) shall be considered.

A straightforward and standards-based architecture that effectively avoids the BSM security manager interaction with NAT gateways (draft-ietf-msec-ipsec-extensions-04.txt, (see bibliography)) is the IPv6 over IPv4 transition mechanism RFC 2529 (see bibliography). In IPv6 over IPv4 (a.k.a. "6over4"), the underlying IPv4 network is treated as a virtual multicast-capable Local Area Network. The IPv6 traffic tunnels over that IPv4 virtual link layer.

Applying BSM security system (with IPsec) in a 6over4 architecture leverages the fact that an administrative domain deploying BSM security system would already be planning to deploy IPv4 multicast router(s). The group's IPv6 multicast routing can execute in parallel to IPv4 multicast routing on that same physical router infrastructure. In particular, IPv6 multicast routers operating with 6over4 mode enabled on their network interfaces replaces the NAT gateways at administrative domain public/private boundaries.

Within the BSM security system, all references to IP addresses are IPv6 addresses for all security association endpoints and these addresses do not change over the group's lifetime. This yields a substantial reduction in complexity and error cases over the NAT-based approaches. This reduction in complexity can translate into better security.

5.4 Summary of multicast key management requirements

In general, multicast services have the following key-management requirements (these requirements however are not intended to be an exhaustive list nor applicable to all applications and services):

1) Group members receive Security Associations (SAs) which including encryption keys, authentication/integrity keys, cryptographic policy that describes the keys, and attributes such as an index for referencing the SA or particular objects contained in the SA. SAs were described in clause 5.1.2.

2) In addition to the policy associated with group keys, the Group Controller (GC) may define and enforce group membership, key management, data security, and other policies that may or may not be communicated to the entire membership.

3) Keys will have a predetermined lifetime and may be periodically refreshed.

4) Key materials should be delivered securely to members of the group so that they are secret, integrity-protected, and verifiably obtained from an authorized source.

5) The key management protocol should be secure against replay attacks and Denial of Service (DoS) attacks.

6) The protocol should facilitate addition and removal of group members. Members who are added may optionally be denied access to the key material used before they joined the group, and removed members should lose access to the key material following their departure.

7) The protocol should support a scalable group rekeying operation without unicast exchanges between members and a GC, to avoid overwhelming a GC managing a large group.

8) The key management protocol should offer a framework for replacing or renewing security transforms, authorization infrastructure and authentication systems.

9) The key management protocol should be secure against collusions among excluded members and non-members. In other words, combining the knowledge of the colluding entities shall not result in revealing additional group secrets.

10) The key management protocol should provide a mechanism to securely recover from a compromise of some or all of the key material.

11) The key management protocol may need to address real-world deployment issues such as Network Address Translation (NAT)-traversal and interfacing with legacy authentication mechanisms. It should be flexible for use at any layer of the protocol stack such as satellite link layer, IP layer or above. Example BSM security cases with satellite link layer security and IPsec are presented in clause 6.

Some of the above requirements are illustrated in the secure multicast scenarios in clause 4 such the enforcement of group rules using policies, dynamic group membership and protection against DoS and replay attacks.

In addition for scenarios 2 and 3 (static or dynamic), if IPsec is used, then the BSM secure multicast management system requires that the IPsec subsystem shall support unidirectional Group Security Associations (GSA). As such only one group member authorized to transmit (Ingress ST or Hub) can use this type of group security association to enforce that group policy. In the inverse direction (e.g. egress STs), the GSA does not have a SAD entry, and the SPD configuration is optionally setup to discard unauthorized attempts to transmit unicast or multicast packets to the group. Similar procedures can be used for link layer security systems such as DVB-RCS.

Regarding scenario 4 (multiple senders), all (or a large subset) of the Group Members are authorized as multicast ingress STs. In such service model, creating a distinct SA with anti-replay state for every potential source ST does not scale to large groups. The group MAY share one SA for all of its ingress STs. In this case, the SA shall NOT use the anti-replay protection service for the multicast data flow to the Group Receivers (egress STs).

6 BSM Multicast Security Functional Architecture Definition

Satellite Independent Service Access Point (SI-SAP) is defined in TS 102 292 [2] and TR 101 984 (see bibliography) as shown in Figure 11.

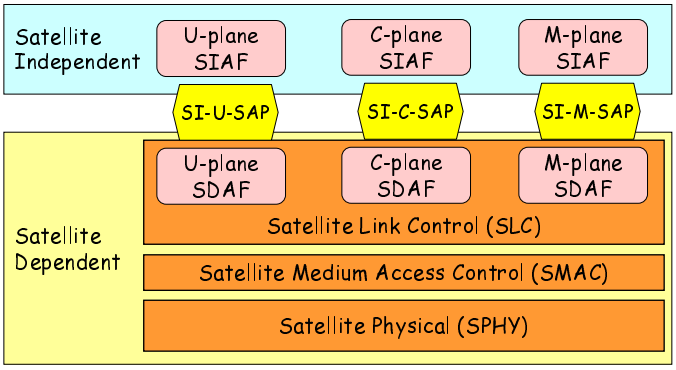


Figure 11: Satellite Independent Service Access Point (SI-SAP)

The SI-SAP and the associated adaptation functions can be logically divided into U-plane, C-plane and M-plane services. These adaptation functions are defined to provide a mechanism for adapting to and from the SI-SAP services:

- The Satellite Independent Adaptation Functions (SIAF) operate at the bottom of Layer 3 to adapt the layer 3 protocols to and from the BSM bearer services.
- The Satellite Dependent Adaptation Functions (SDAF) operate at the top of Layer 2 to adapt the BSM bearer services to and from the native air interface services.

The BSM multicast security architecture elements are defined in this clause together with the detailed interactions across the SI-SAP interface in the U-plane, C-plane and M-plane. Also interactions with BSM entities (such as QoS and multicast source management) are addressed.

6.1 Detailed BSM security functional architecture

The BSM general security architecture document (TS 102 465 [1], clause 6) defines the BSM architecture elements and interactions across the SI-SAP interface. The same architecture applies to secure multicast over BSM. If a unicast session is present in combination with multicast (such as unicast satellite return channel or a multicast ingress ST forwarding data to ingress Hub) the security procedures presented in the BSM general security architecture document (TS 102 465 [1]) shall be applied.

In this clause, the focus of the functional architecture is the multicast key management exchanges (registration, re-keying and data key distribution as presented in clause 5). The correct relationship between security entities: BSM **Network** security manager (the security key server as presented in clause 4 scenarios), ST **Local** security manager (the security client as presented in clause 4 scenarios), ingress and egress STs shall be enforced by the correct use of security policies, with the strict enforcement of the roles for each entity (e.g. the permissions to send in the multiple senders scenario).

6.1.1 Case 1: Secure multicast in the Satellite Dependent (SD) layer (below SI-SAP)

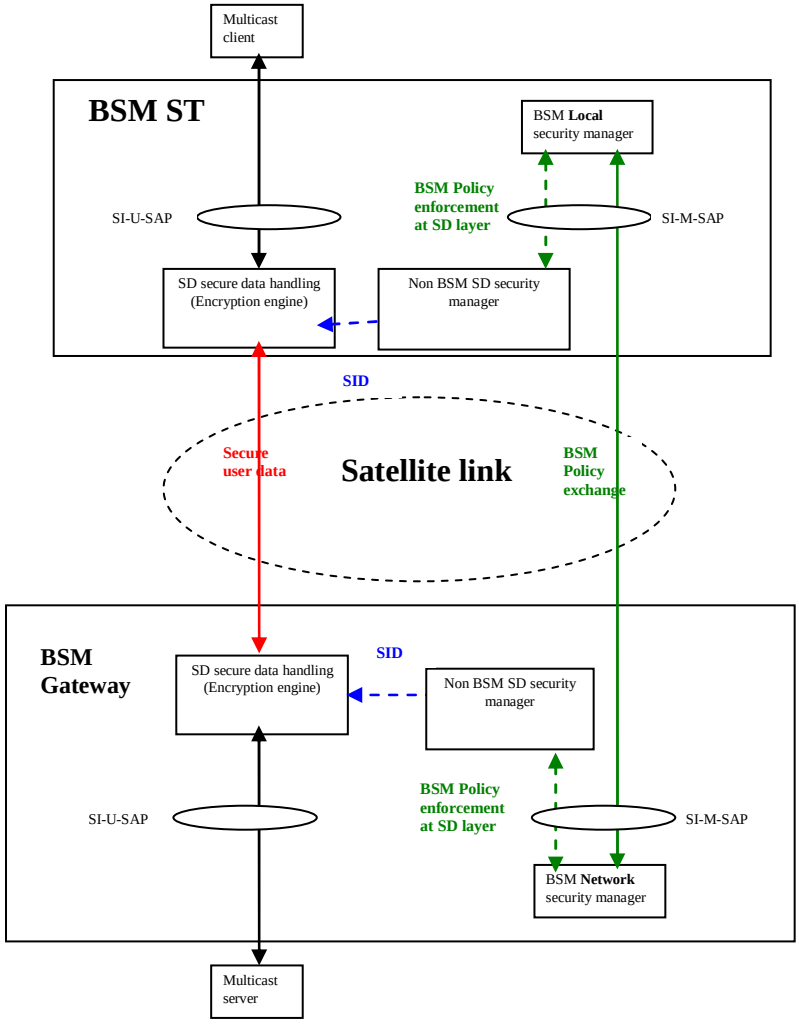


Figure 12: Case 1 Secure link layer multicast with BSM access control

Typical examples of such system are DVB-RCS with MPE or Unidirectional Lightweight Encapsulation (ULE) RFC 4326 IP encapsulation (see bibliography).

This case (Figure 12) is transparent to BSM network. However, the BSM **Local** and **Network** security managers shall be able to enforce the BSM security multicast policy rules. The multicast security policy is distributed through the SI-M-SAP interface.

Using link layer security has the major advantage of authenticating satellite terminals (BSM STs and gateways), which is not possible using security methods above the SI-SAP.

6.1.2 Case 2: Secure multicast with network layer security (above SI-SAP)

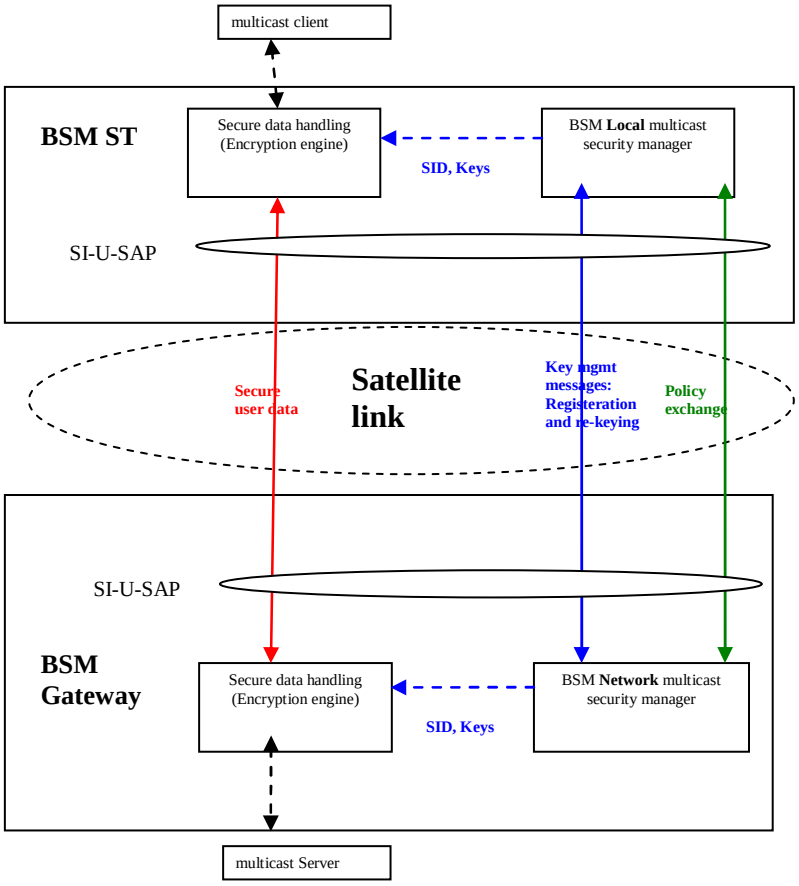


Figure 13: Case 2 Using network layer (IPsec) for BSM multicast security

As shown in Figure 13, this case illustrates the use of network layer security (such as IPsec) for secure multicast over BSM network in a security gateway-to-gateway configuration such as VPN over satellites scenario. IPsec protocol operates above the SI-SAP.

Security is provided between a security gateways (that can be co-located with a BSM ST or Gateway). The security gateway consists of three functional entities:

1) Secure data handling entity (privacy/integrity engine): IPsec shall operate in tunnel mode. The data security protocol was described in clause 5.1.3.3.

2) key management entity: In a star topology, there is a **Network** security manager for the whole BSM network (co-located with BSM gateway/hub). In addition there is a **Local** security manager in each ST. The key management protocols such as registration and rekeying were described in clauses 5.1.3.1 and 5.1.3.2.

3) Security policy client and server and distribution mechanism as descried in clause 5.1.4.

Figure 13 shows that the SI-U-SAP (the user interface) ONLY is used to communicate all secure information (user data key management messages and multicast security policies).

Any of the key multicast key management systems described in clause 5.1.5 can used here. The Security Association Identity SID shall be used in all security management message exchanges.

The client/server authentication/authorization processes is not shown here. However it is similar to the procedures described in clause 6 of TS 102 465 [1].

6.1.3 Case 3: Mixed secure multicast (security manager above SI-SAP and security engine below SI-SAP)

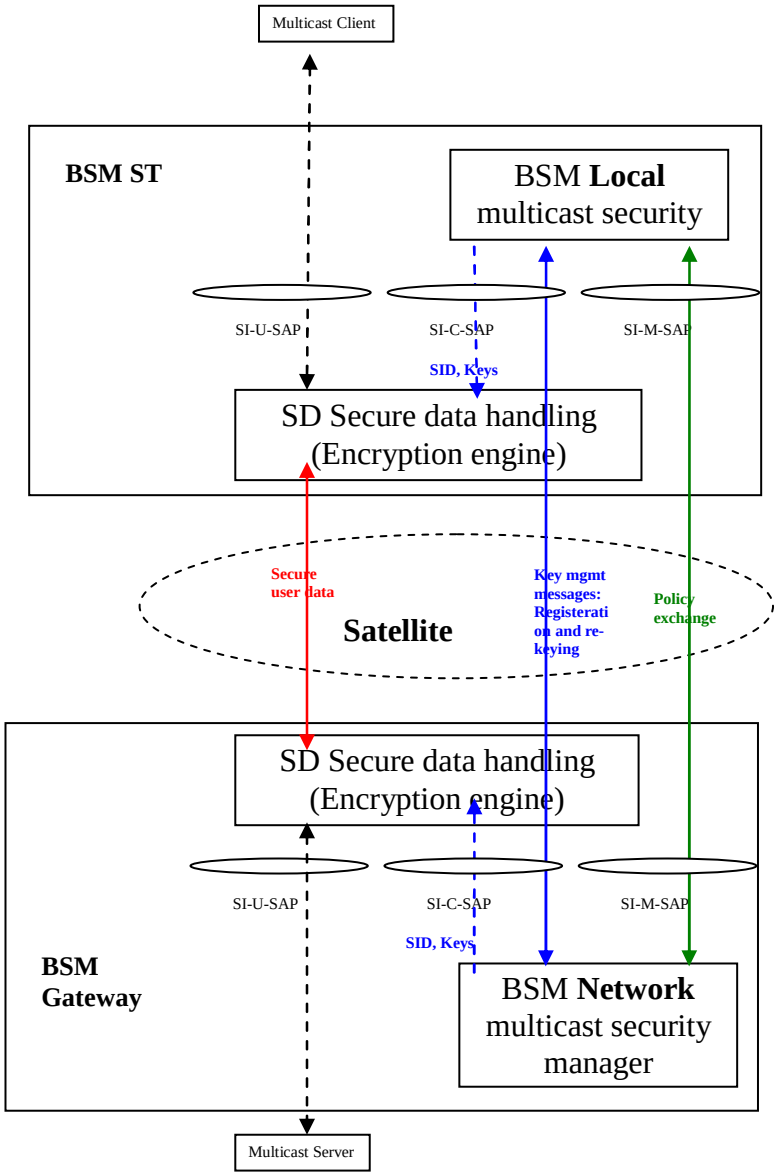


Figure 14: Case 3 Mixed layers BSM multicast security

As shown in Figure 14, this case illustrates the use of link layer security (below SI-SAP) for data security (clause 5.1.3.3). The security manager is above the SI-SAP for the multicast key management (clauses 5.1.3.1 and 5.1.3.2). This can be star or mesh topology with a centralized security key management.

Typical examples of such system are DVB-RCS (see EN 301 790 in bibliography) with MPE or Unidirectional Lightweight Encapsulation (ULE) RFC 4326 IP encapsulation. Annex A show more details of DVB-RCS key management as an application layer protocol.

Like case 2, security is provided between a security gateways (that can be co-located with BSM ST or Gateway). The security gateway consists of three functional entities:

1) Secure data handling entity (privacy/integrity engine): IPsec shall operate in tunnel mode. The data security protocol was described in clause 5.1.3.3.

2) key management entity: In a star topology, there will a **Network** security manager for the whole BSM network (co-located with BSM gateway/hub). In addition there is a **Local** security manager in each ST. The key management protocols such as registeration and rekeying were described in clauses 5.1.3.1 and 5.1.3.2.

3) Security policy client and server and distribution mechanism as descried in clause 5.1.4.

Figure 14 shows that the SI-U-SAP (the user interface) is used to communicate secure user data. While the key management secure information is passed through the SI-C-SAP interface. The SI-M-SAP (management interface) is used to pass the multicast security policies between the BSM **Network** and STs **Local** security manager.

The specific satellite systems (SD layer) security shall be used. For example, for DVB-RCS satellite systems, the logon and key exchanges procedures of DVB-RCS recommendations (see EN 301 790 in bibliography) shall be used to establish all security associations (annex A provides more details for this procedure). For BSM systems operating with ULE, then the ULE specific key management procedures shall be used (see IETF documents in bibliography). This will ensure the mutual authentication between all security entities, establishing the keys used subsequently to secure the user data. Using link layer security will also authenticate BSM terminals (STs and gateways), which is not possible with using IPsec (case 2).

The Security association identity SID shall be used in all security management message exchanges.

Similar to case 2, the client/server authentication/authorization processes is not shown here. However it is similar to the procedures described in clause 6 in TS 102 465 [1].

6.1.4 Case 4: End-to-end secure multicast

This case is used to transport non-BSM secure multicast traffic over the BSM network. It is transparent to BSM security system, except applying access control on such traffic. As shown in Figure 15, the multicast security policy is used to enforce the BSM security rules. Again the SI-M-SAP is used for policy distribution.

The BSM multicast traffic manager is responsible for grant or deny access to such external traffic. The BSM multicast source management, as described in details in TS 102 461 [6]. Also more detailed interaction between security and source management is presented in clause 6.3.

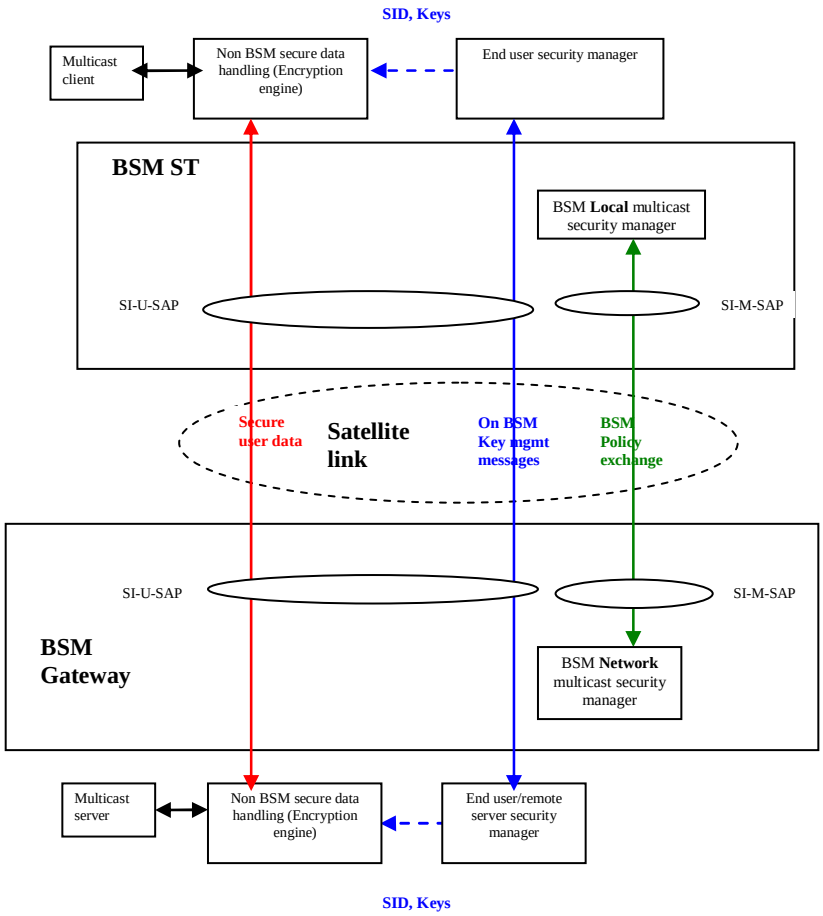


Figure 15: Case 4 Secure end-to-end multicast with BSM access control

6.1.5 Case 5: Secure multicast in composite groups (BSM and non-BSM membership)

As shown in Figure 16, this case illustrates the BSM architecture and interactions through the SI-SAP interface for a secure composite group (cryptographically heterogeneous multicast group). Composite groups overview is presented in annex C and brief scenario was shown in scenario 5 in clause 4.2.5. An example of this scenario is a multicast group that spans several security domains such as a BSM network and another terrestrial Internet domain.

In Figure 16, we assume the use of IPsec for both BSM domain (*domain 1*) and non BSM security domain (*domain 2*). IPsec protocol operates above the SI-SAP.

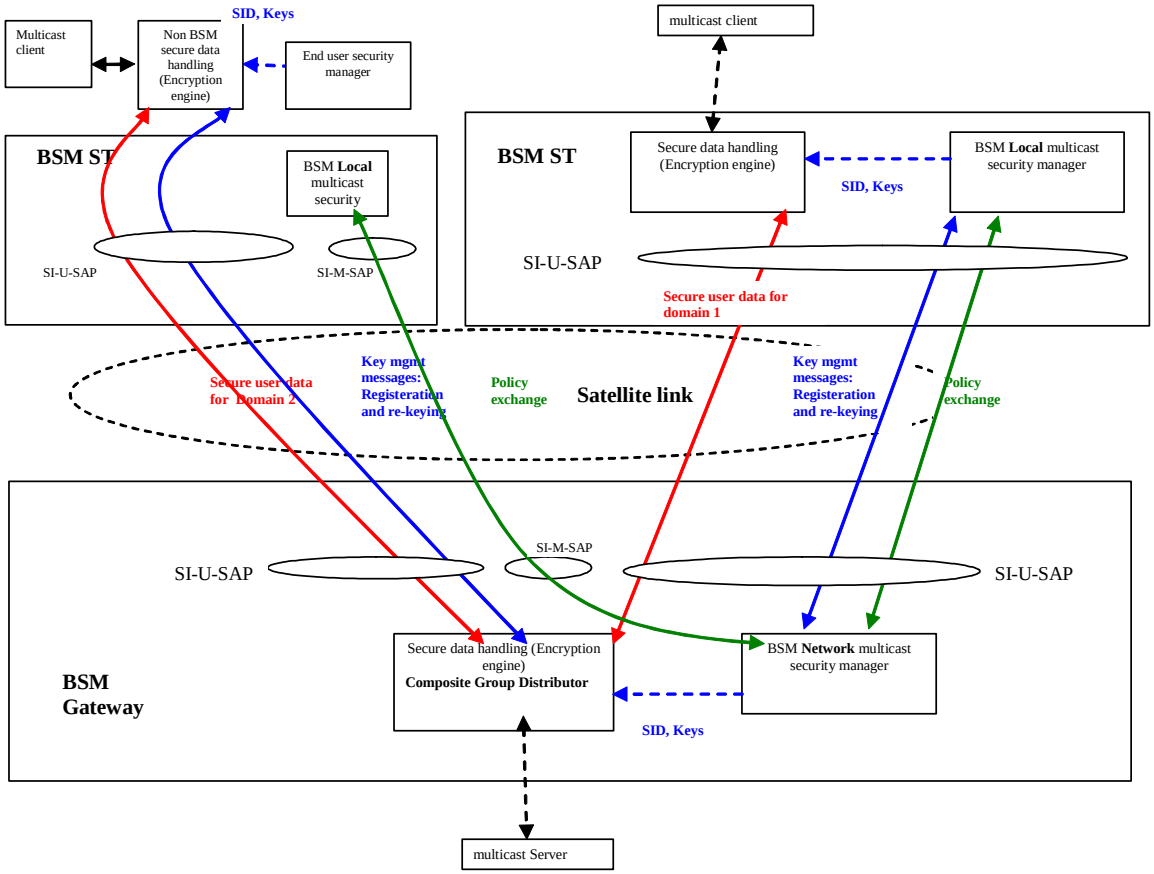


Figure 16: Case 5 Using network layer for BSM composite groups

Case 5 can be considered as combination of case 2 (IPsec, clause 6.1.2) for domain 1 operations and case 4 (end-to-end, clause 6.1.4) for domain 2 operations. The main difference with case 4 is that the secure multicast traffic is generated within the BSM network (transmitted through the BSM Ingress Gateway) for domain 2. The Composite group distributor generates the secure multicast traffic for both domains 1 and 2. The egress ST (in domain 2) does not play any role in the security process except access control (through the use of security policies (as shown in Figure 16).

6.2 Interactions between multicast security and QoS BSM entities

6.2.1 QoS provisioning for key management messages

This clause make use of the BSM general QoS architecture and interworking with RSVP and Diffserv that are presented in detailed in TS 102 462 [7], TS 102 463 [3] and TS 102 464 [5] respectively.

Reliability of key management messages is important for the efficient working of secure multicast in BSM networks. If RSVP or DiffServ are used for QoS provisioning, then key management messages should be transport in a better than best effort flows. For example, Figure 17 shows the transport of these messages in a Guaranteed Service (GS) flow.

In the case of DiffServ the security policies shall be defined in the SLA. The Common Open Policy Service (COPS) protocol can used to carry QoS or security information between BSM management entities and satellite terminals (gateways/ST) (RFC 2748 (see bibliography)) and to update them dynamically (even in the case of DiffServ). In addition, if COPS is used for QoS provisioning, then COPS Policy Provisioning protocol (COPS-PR) can be used for security policy transfer (RFC 3084, (see bibliography)). The transport of security message flows shall be defined in the QoS policy at the time of service provisioning setup.

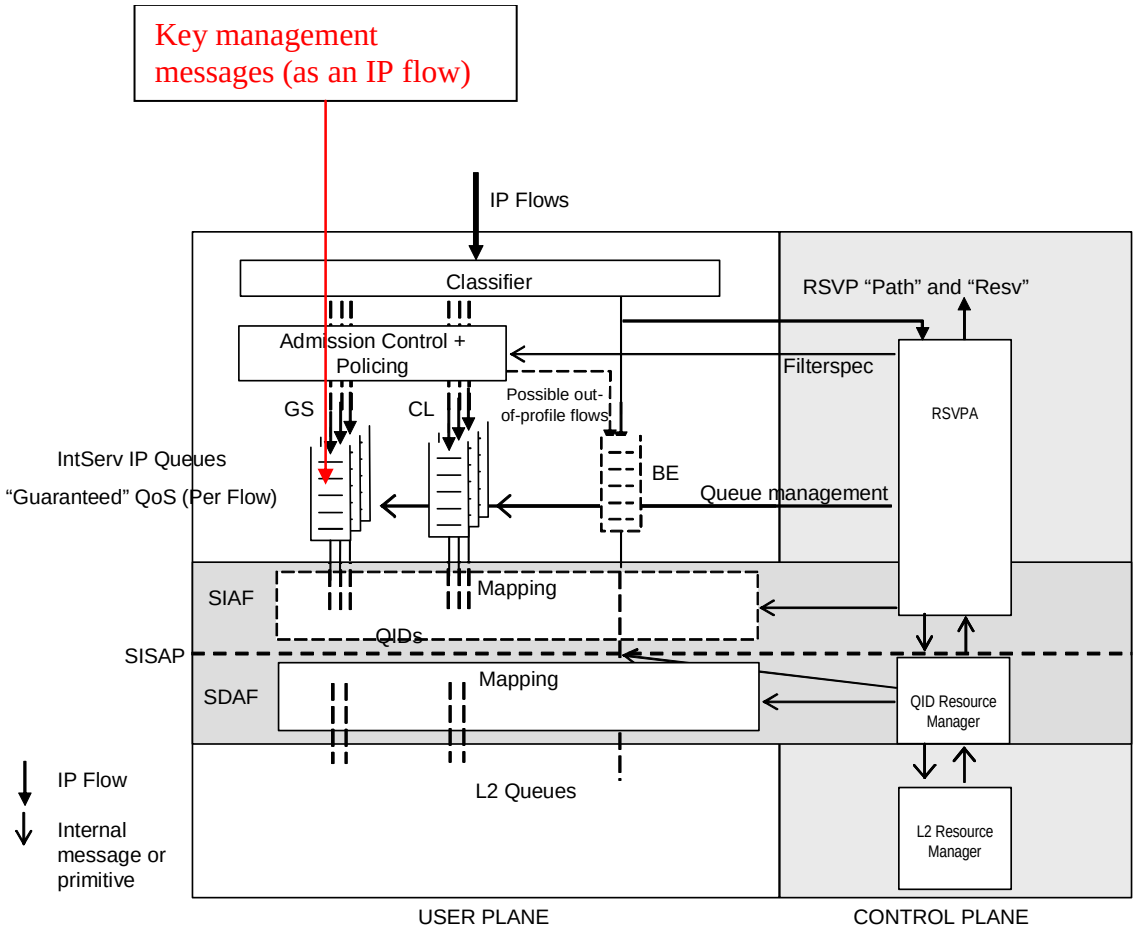


Figure 17: Example Security messages mapping in ingress QoS Architecture (Dynamic SD Resources)

6.2.2 Securing RSVP and Diffserv message exchanges

Another interaction between security and QoS in BSM network is the security and authenticity of QoS signalling between NCC, ingress and egress STs. TS 102 463 [3] describes a centralized and distributed RSVP architectures. Figure 18 shows the centralized architecture as an example.

Securing RSVP messaging using IPsec has several complications as presented in RFC 4230 (see bibliography). Therefore, the use of IPsec (above the SI-SAP) is not recommended. Optionally security can be applied to the QoS control message exchanges (below the SI-SAP) between the NCC and ingress ST (Figure 18). If security is required, then case 1 or 3 (clause 6.1.1 or 6.1.3) can used, where the SD layer security (e.g. using authentication and/or encryption) is applied.

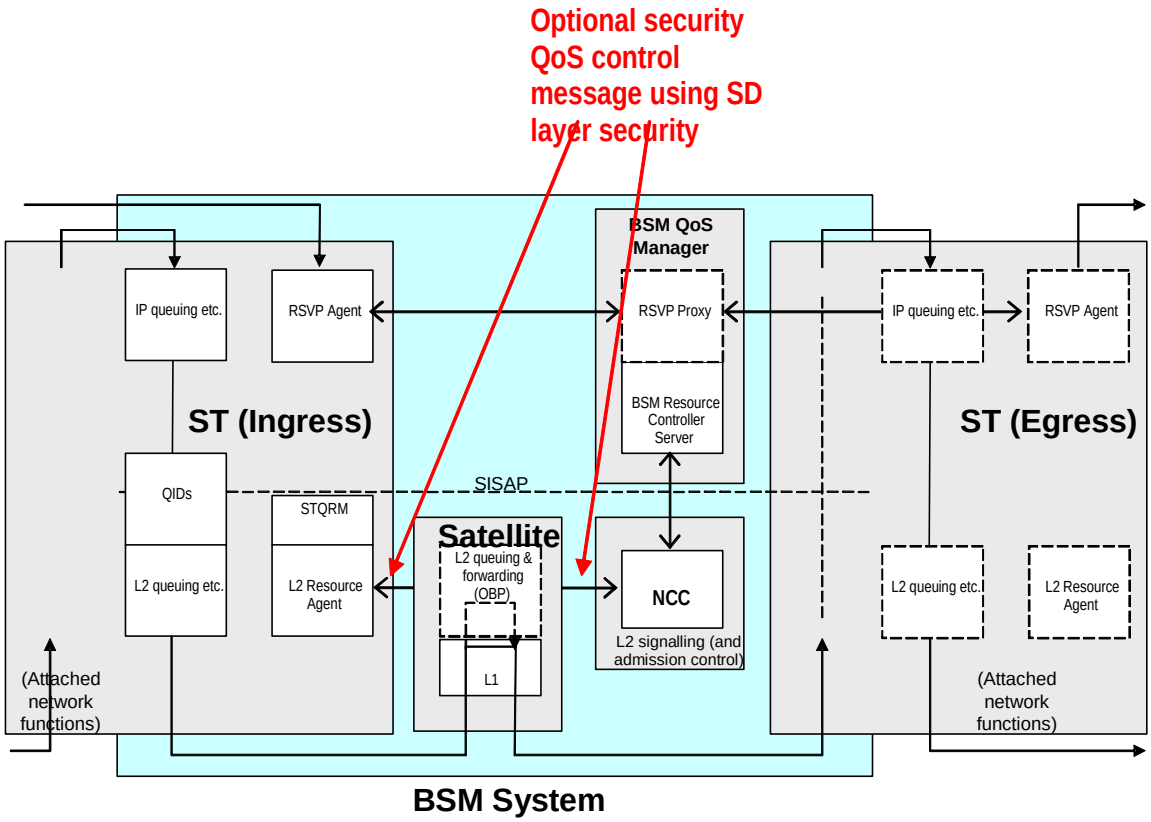


Figure 18: Secure QoS signalling in BSM centralized RSVP Architecture (Dynamic SD Resources)

The security policy shall define the security services needed for QoS signalling at the time of service provisioning setup. The choices for QoS signalling messages are:

- No security.
- Authentication only.
- Authentication and encryption.

In case of static DiffServ, or dynamic DiffServ without explicit signalling (such as RSVP or NSIS) QoS signalling is not provided at IP layer. The IP queues are limited to a small number (maximum number is 64), and they are usually static or slowly-changing (on a time scale of hours or days). So the control plane operation do not need any BSM specific security considerations. The following way of operating (described in TS 102 464 [5]) shows that, even in case of dynamic DiffServ, messages in the control-plane are only exchanged below the SI-SAP (Figure 19):

1) The IP resource manager interacts with the IP classifier and queuing module in the user-plane and with external IP signalling (optional) to understand when and whether new resources are needed (or not needed anymore). The IP DiffServ queues may remain static, but the traffic situation might change.

   MESSAGES: (1a) terminal defined, (1b) standard IP signalling, e.g. RSVP, NSIS.

2) So if the situation changes this module should notify the STQRM and take appropriate actions to allocate/release resources at the SD layers.

   MESSAGES: (2) SI-SAP primitives.

3) This triggers an exchange of messages along the red lines, down to the SD layer and the NCC, since the resources at the SD layer will be, most likely, centrally managed.

   MESSAGES: (3a) terminal defined, (3b) BSM defined.

4) The reply of the NCC will follow the green lines up to the IP resource manager.

   MESSAGES: (4a) BSM defined, (4b) terminal defined, (4c) SI-SAP primitives.

5) These replies will enable the (re)configuration of the queue structure and of the mapping shown in TS 102 463 [3].

   MESSAGES: (5a) terminal defined, (5b) terminal defined, (5c) terminal defined.

6) In the end these operations might trigger responses at IP signalling level (optional).

   MESSAGES: (6) standard IP signalling e.g. RSVP, NSIS.

Since these messages exchanges between the ST and NCC in the in SD layer, Optional security service may be applied. If security is required, then case 1 or 3 (clause 6.1.1 or 6.1.3) can used, where the SD layer security (e.g. using authentication and/or encryption) is applied to the messages 3b and 4a in Figure 19.

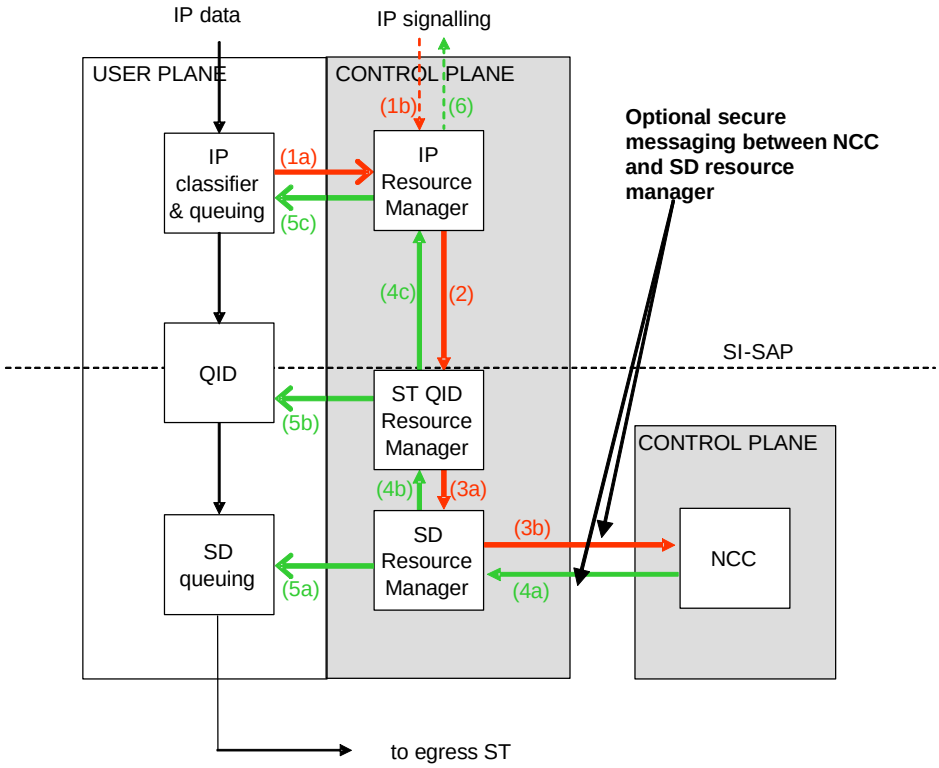


Figure 19: Control-Plane operations of a DiffServ-aware ST - BSM security interactions

6.3 Interactions between multicast security and multicast source management entities

As presented in TS 102 461 [6], BSM Multicast Source Management refers to the combination of Multicast Traffic Management, Multicast Control Management (using PIM-SM and IGMP) and Multicast Address Management functions to create, maintain and remove BSM multicast distribution trees. Similar to clause 6.2.2, the multicast source management signalling messages can be secured. Therefore and optionally, security can be applied to these signalling message exchanges (below the SI-SAP) between the NCC and ingress/egress ST.

If security is required, then case 1 or 3 (clause 6.1.1 or 6.1.3) can used, where the SD layer security (e.g. using authentication and/or encryption) is applied.

Annex A (informative): The current DVB-RCS security system

The DVB-RCS specification (see EN 301 790 in bibliography) defines the return (or "interaction") channel for communication between a Return Channel Satellite Terminal (RCST) and a Gateway/hub ground station. The term RCST simply refers to a satellite terminal, the term gateway refer to a large ground station that is connected to other networks such as the Internet, and the hub is the entity that is responsible for multiplexing data destined to multiple RCSTs onto the satellite broadcast channels. The gateway and hub station are typically co-located in satellite systems. The satellite network is monitored and controlled by the NCC. Signalling is transmitted between the NCC and the RCSTs over the forward link and the return link.

The DVB-RCS security specification currently supports the authentication of each RCST to the NCC, and the encryption of both forward and return link traffic, and these functions are described in the following clauses.

A.1 DVB-RCS Authentication

Each RCST holds a shared secret key, called a cookie, known only to the given RCST and the NCC. This cookie is used during key exchanges: A logon is initiated by a RCST, for example when the first user of the RCST wishes to use the satellite link for data transfer. This is followed by an initial handshake between the NCC and the RCST to agree the security profile (i.e. the cryptographic algorithms and key sizes to be used): this is performed by the Security Sign-On and Security Sign-On Response messages (Figure A.1). The current DVB-RCS specification supports a single session key per RCST, this key being used to encrypt data traffic in both directions on the satellite link. In the process of authentication, the specification then allows one of three key exchange mechanisms to occur. The objectives of these key exchange messages are firstly to authenticate the RCST and secondly for the RCST and NCC to agree the session key to be used. The three key exchanges and their principal features are as follows:

- Main Key Exchange (MKE): this uses the Diffie-Hellman algorithm to develop a shared secret between the NCC and RCST, known only to these two entities; it also uses the cookie (secret key) held in the RCST to authenticate the RCST to the NCC; optionally it can use the newly developed shared secret to update the cookie; and finally it derives a session key from the newly developed shared secret.
- Quick Key Exchange (QKE): this uses the cookie to authenticate the RCST to the NCC; and derives a session key from the cookie.
- Explicit Key Exchange (EKE): this transmits (encrypted) a key from the NCC to the RCST; this key is then used as the session key.

Following logon, the NCC can initiate further key exchanges as required to update the session key.

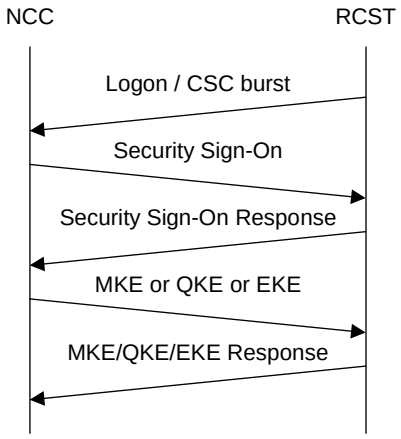


Figure A.1: DVB-RCS security establishment

A.2 Transport of security messages

The MAC security messages transmitted over the air interface can be transported:

- Either using DULM (see EN 301 790 in bibliography) over the return path and using a dedicated and well-known PID over the forward path. "Security enhanced" RCSTs will thus have to MAC-filter this PID.
- Or using the same IP communication stack carrying the user and management traffic in the DVB-RCS network as shown in Figure A.2 Security messages are inserted in UDP datagrams with TLV descriptors (Figure A.3), with the possibility to have several security messages per datagram.

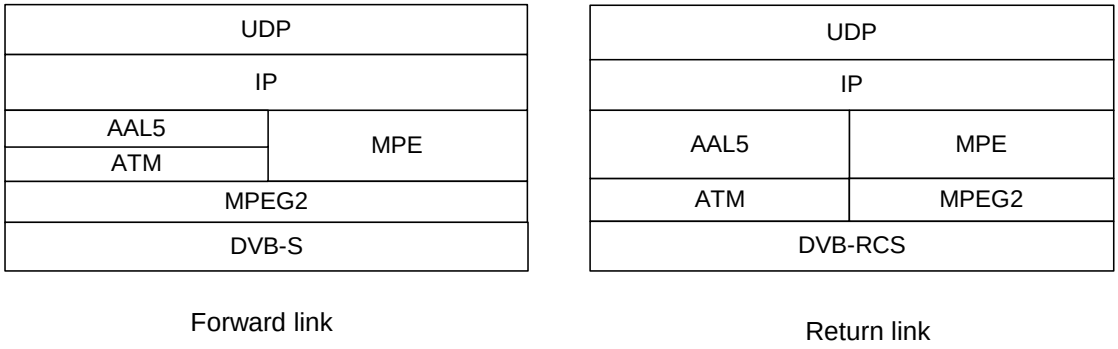


Figure A.2: IP protocol stack for transporting security messages

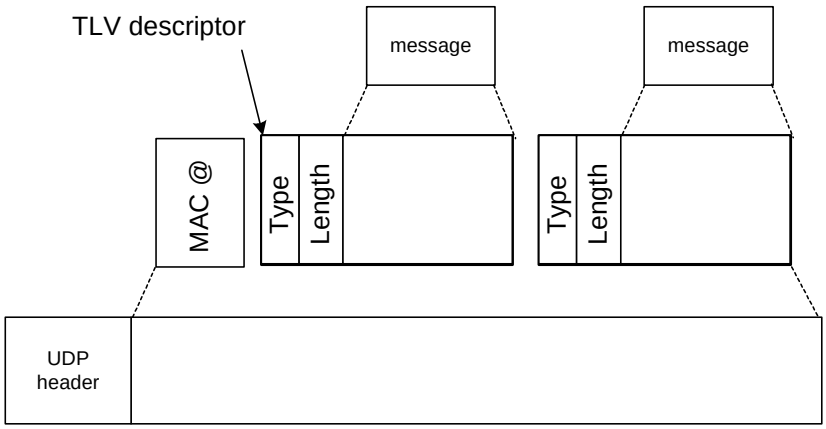


Figure A.3: Several security messages per datagram

For message transfers from a RCST to the NCC, the RCST's MAC address is inserted at the beginning of the UDP payload, as illustrated in Figure A.3. This MAC address allows the NCC to know from which RCST the messages are coming.

TLV descriptors allow to identify the type of the security messages with the following syntax:

Table A.1: TLV descriptor structure

Security_TLV_descriptor {	Bytes	Parameter
Type	1	
Length	1	Mlen

If (Type == 0x0d) {
EKE message
}
if (Type == 0x35) {
Sign On message
}
	
	Mlen
	
	Mlen	

In table A.1, the **EKE message** field can be either an EKE request message or an EKE response message, depending which entity sends it (NCC or RCST). The same remark applies to the **Sign On message** field.

The **Length** field is the length in bytes of the **EKE message** or **Sign On message** field.

A.3 DVB-RCS multicast extensions

The current DVB-RCS standard supports the following security requirements:

- Enables RCST authentication to NCC, by means of a logon phase.
- Maintains the forward and return uplinks and downlinks secure from eavesdropping, either by unauthorized persons or by other users of the satellite system, provided "individual user scrambling" is implemented.
- Supports separate keys for unicast traffic to each RCST so that no RCST can decrypt unicast traffic intended for a different RCST.
- Supports periodic rekeying of unicast channels using the EKE messages.
- Supports logout.

The security procedure in the current DVB-RCS standard (as presented above) has several gaps regarding multicast security. The standard currently mentions the use of Explicit Key Exchange (EKE) for multicast (see EN 301 790 in bibliography). However it is not clear how a particular key exchanged with EKE can be linked to multicast in general or to a particular multicast service, since only one key is used per session and this key needs to support all unicast and multicast traffic through the RCST. In particular, in order to support multicast security the following additional requirements can be stated:

- Support separate keys for each multicast channel.
- Transmit multicast keys efficiently to RCSTs.
- Support different security profiles (i.e. a specific set of cryptographic algorithms and parameters) for each channel's keys, both unicast and multicast.
- Support periodic rekeying of multicast channels - this is usually performed at regular intervals to reduce the probability of successful cryptanalysis of the encrypted traffic.
- Support rekeying to perform ejection of a compromised member of a multicast group.

In order to support multiple keys per RCST, the Main Key Exchange (MKE), Quick Key Exchange (QKE) and Explicit Key Exchange (EKE) messages need to both support multiple keys and also identify which unicast or multicast channel uses a given key. These messages therefore need extending to allow this. One of the following two mechanisms can be adopted to enable the NCC to send the keys for each multicast group to an RCST:

- At logon: keys for all multicast groups are distributed to each RCST, at the same time as the RCST's individual (unicast) session key. This mechanism is suitable where there are a small number of multicast groups. The advantage of this mechanism is its simplicity, but the disadvantage is that if there are a large number of multicast keys and each RCST is only expected to join a small number of groups then a large amount of network capacity is wasted in sending unwanted keys.
- On demand: keys for multicast groups are issued on demand, when the RCST joins a multicast group. This mechanism is scalable and suitable for systems with a large number of multicast groups, and requires new message types to enable a RCST to request the key(s).

In addition, in order to provide periodic rekeying and existing member ejection, the MKE/QKE/EKE messages can be used. However, key management architectures exist that are highly scalable to large multicast groups; one particularly promising mechanism which is receiving a high degree of interest is Logical Key Hierarchy (LKH) RFC 2627 (see bibliography). LKH requires that multiple keys be unicast to each RCST when it joins a multicast group, and that some further keys be multicast to the group when rekeying takes place. LKH therefore requires two new extensions to the EKE message, which we call Extended EKE and Rekey EKE.

Therefore four sets of DVB-RCS security specification amendments, can be considered to support secure multicast:

- Support for multiple keys per RCST, to enable unicast and multicast traffic to use separate keys.
- Transmission of multicast keys at logon.
- RCST on-demand request for keys, to provide a scalable mechanism for multicast group joining.
- Extensions to EKE to support multicast rekeying, to enable key updates in case an RCST is compromised (Extended EKE and Rekey EKE).

Annex B (informative): IPSec extensions for multicast

The majority of the secure IP multicast work is carried within the IETF. There is a limited overview of the secure multicast issues over satellites in IABG Final report (see bibliography) and in draft-cruickshank-ipdvb-sec-req-04.txt (see bibliography). A security gateway implementation of IPsec shall use tunnel mode. Such usage has the following disadvantages:

- There is an extra overheads associated with using IPsec in tunnel mode, i.e. the extra IP header (IPv4 or IPv6).
- Multicast is considered as a major service over satellite links. The current IPsec specifications [RFC 4301] only define a pairwise tunnel between two IPsec devices with manual keying.
- There is a need to protect the identity (NPA) of Satellite Receivers; IPsec is not suitable for providing this service.

draft-ietf-msec-ipsec-extensions-04.txt (see bibliography) is work in progress in defining the extra detail needed for IPsec to work efficiently with multicast. The Security Architecture for the Internet Protocol RFC 4301 (see bibliography) describes security services for traffic at the IP layer. That architecture primarily defines services for Internet Protocol (IP) unicast packets, as well as manually configured IP multicast packets. The draft-ietf-msec-ipsec-extensions-04.txt (see bibliography) further defines the security services for manually and dynamically keyed IP multicast packets within that Security Architecture.

B.1 Security Association Modes

IPsec supports two modes of use: transport mode and tunnel mode. In transport mode, IP Authentication Header (AH) RFC 4302 (see bibliography) and IP Encapsulating Security Payload (ESP) RFC 4303 (see bibliography) provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets. A host implementation of IPsec using the multicast extensions MAY use either transport mode and tunnel mode to encapsulate an IP multicast packet. These processing rules are identical to the rules described in RFC 4301 (see bibliography). However, the destination address for the IPsec packet is an IP multicast address, rather than a unicast host address.

A security gateway implementation of IPsec using the multicast extensions shall use a tunnel mode SA, for the reasons described in RFC 4301 (see bibliography). In particular, the security gateway shall use tunnel mode to encapsulate incoming fragments, since IPsec cannot directly operate on fragments.

B.1.1 Tunnel Mode with Address Preservation

New header construction semantics are required when tunnel mode is used to encapsulate IP multicast packets that are to remain IP multicast packets. This is due to the following unique requirements of IP multicast routing protocols (e.g. PIM-SM RFC 2362 (see bibliography)):

- IP multicast routing protocols compare the destination address on a packet to the multicast routing state. If the destination of an IP multicast packet is changed it will no longer be properly routed. Therefore, an IPsec security gateway shall preserve the multicast IP destination address after IPsec tunnel encapsulation. The GKM Subsystem on a security gateway implementing the IPsec multicast extensions preserves the multicast IP address as follows. Firstly, the GKM Subsystem sets the Remote Address PFP flag in the GSPD-S entry for the traffic selectors. This flag causes the remote address of the packet matching IPsec SA traffic selectors to be propagated to the IPsec tunnel encapsulation. Secondly, the GKM Subsystem needs to signal that destination address preservation is in effect for a particular IPsec SA. The GKM protocol shall define an attribute that signals destination address preservation to the GKM Subsystem on an IPsec security gateway.

- IP multicast routing protocols also typically create multicast distribution trees based on the source address. If an IPsec security gateway changes the source address of an IP multicast packet (e.g. to its own IP address), the resulting IPsec protected packet may fail RPF checks on other routers. A failed RPF check may result in the packet being dropped. To accommodate routing protocol RPF checks, the GKM Subsystem on a security gateway implementation implementing the IPsec multicast extensions shall preserve the original packet IP source address as follows. Firstly, the GSPD-S entry for the traffic selectors shall have the Source Address PFP flag set. This flag causes the remote address to be propagated to the IPsec SA. Secondly, the GKM Subsystem needs to signal that source address preservation is in effect for a particular IPsec SA. The GKM Subsystem SHALL define a protocol attribute that signals source address preservation to the GKM Subsystem on an IPsec security gateway.

In summary, retaining both the IP source and destination addresses of the inner IP header allow IP multicast routing protocols to route the packet irrespective of the packet being IPsec protected. This result is necessary in order for the multicast extensions to allow a security gateway to provide IPsec services for IP multicast packets. This variation of RFC 4301 (see bibliography) tunnel mode is known as "tunnel mode with address preservation".

B.2 Modifications to IPsec Databases

The following clauses describe the GKM Subsystem and IPsec extension interactions with the major IPsec databases. The major IPsec databases needed expanded semantics to fully support multicast.

Group Security Policy Database (GSPD)

The Group Security Policy Database is a security policy database capable of implementing both unicast security associations as defined by RFC 4301 (see bibliography) and the multicast extensions defined by the present document. A new Group Security Policy Database (GSPD) attribute is introduced: GSPD entry directionality.

Directionality can take three types. Each GSPD entry can be marked "symmetric", "sender only" or "receiver only". Symmeric GSPD entries are the common entries as specified by RFC 4301. Symmetric SHOULD be the default directionality unless specified otherwise. GSPD entries marked as "sender only" or "receiver only" SHOULD support multicast IP addresses in their destination address selectors. If the processing requested is bypass or discard and a sender only type is configured the entry SHOULD be put in GSPD-O only. Reciprocally, if the type is receiver only, the entry SHOULD go to GSPD-I only. SSM is supported by the use of unicast IP address selectors as documented in RFC 4301.

Security Association Database (SAD)

The Security Association Database (SAD) can support multicast SAs, if manually configured. An outbound multicast SA has the same structure as a unicast SA. The source address is that of the Group Speaker and the destination address is the multicast group address. An inbound multicast SA shall be configured with the source addresses of each Group Speaker peer authorized to transmit to the multicast SA in question. The SPI value for a multicast SA is provided by a GCKS, not by the receiver as occurs for a unicast SA. Other than the SPI assignment and the inbound packet de-multiplexing described in RFC 4301 section 4.1, the SAD behaves identically for unicast and multicast security associations.

Peer Authorization Database (PAD)

The Peer Authorization Database (PAD) needs to be extended in order to accommodate peers that may take on specific roles in the group. Such roles can be GCKS, Group Speaker (in case of SSM) or a Group Receiver. A peer can have multiple roles. The PAD may also contain root certificates for PKI used by the group.

B.3 Data Origin Authentication

As defined in RFC 4301 (see bibliography), data origin authentication is a security service that verifies the identity of the claimed source of data. A Message Authentication Code (MAC) is often used to achieve data origin authentication for connections shared between two parties. But MAC authentication methods are not sufficient to provide data origin authentication for groups with more than two parties. With a MAC algorithm, every group member can use the MAC key to create a valid MAC tag, whether or not they are the authentic originator of the group application's data.

When the property of data origin authentication is required for an IPsec SA distributed from a GKCS, an authentication transform where the originator keeps a secret should be used. Two possible algorithms are TESLA RFC 4082 or RSA digital signature RFC 4359 (see bibliography). In some cases, (e.g. digital signature authentication transforms) the processing cost of the algorithm is significantly greater than an HMAC authentication method. To protect against denial of service attacks from device that is not authorized to join the group, the IPsec SA using this algorithm may be encapsulated with an IPsec SA using a MAC authentication algorithm. However, doing so requires the packet to be sent across the IPsec boundary for additional inbound processing RFC 4301 (see bibliography). This use of ESP encapsulated within ESP accommodates the constraint that an ESP trailer defines an Integrity Check Value (ICV) for only a single authenticator transform. Relaxing this constraint on the use of the ICV field is an area for future standardization.

B.4 Interworking between unicast and multicast Key Management

Often, the GKM subsystem will be introduced to an existent IPsec subsystem as a companion key management protocol to IKEv2 RFC 4306 (see bibliography). A fundamental GKM protocol IP Security subsystem requirement is that both the GKM protocol and IKEv2 can simultaneously share access to a common Group Security Policy Database and Security Association Database. The mechanisms that provide mutually exclusive access to the common GSPD/SAD data structures are a local matter. This includes the GSPD-outbound cache and the GSPD-inbound cache.

However, it should be noted that IKEv2 SPI allocation is entirely independent from GKM SPI allocation because group security associations are qualified by a destination multicast IP address and may optionally have a source IP address qualifier. See RFC 4303 (see bibliography) for further explanation. The Peer Authorization Database does require explicit coordination between the GKM protocol and IKEv2.

B.5 IPv4 NAT issues

With the advent of NAT and mobile Nodes, IPsec multicast applications shall overcome several architectural barriers to their successful deployment. This clause surveys those problems and identifies the GSPD/SAD state information that the GKM protocol shall synchronize across the group membership:

GSPD Losses Synchronization with Internet Layer's State

The most prominent problem facing GKM protocols supporting IPsec is that the GKM protocol's group security policy mechanism can inadvertently configure the group's GSPD traffic selectors with unreliable transient IP addresses. The IP addresses are transient because of Network Address Translation (NAT), which can unilaterally change a multicast speaker's source IP address without signalling the GKM protocol. The absence of a GSPD synchronization mechanism can cause the group's data traffic to be discarded rather than processed correctly.

SSM Routing Dependency on Source IP Address

Source-Specific Multicast (SSM) routing depends on a multicast packet's source IP address and multicast destination IP address to make a correct forwarding decision. However, a NAT gateway alters that packet's source IP address as its passes from a private network into the public network. This alteration in the source IP address makes it infeasible for transit multicast routers in the public Internet to know which SSM speaker originated the multicast packet, which in turn selects the correct multicast forwarding policy.

ESP Cloaks Its Payloads from NAT Gateway

When traversing NAT, application layer protocols that contain IPv4 addresses in their payload need the intervention of an Application Layer Gateway (ALG) that understands that application layer protocol RFC 3027, RFC 3235 (see bibliography). The ALG massages the payload's private IPv4 addresses into equivalent public IPv4 addresses. However, when encrypted by end-to-end ESP, such payloads are opaque to application layer gateways.

When multiple Group Speakers reside behind a NAT with a single public IPv4 address, the NAT gateway can not do UDP or TCP protocol port translation (i.e. NAPT) because the ESP encryption conceals the transport layer protocol headers. The use of UDP encapsulated ESP RFC 3948 (see bibliography) avoids this problem. However, this capability shall be configured at the GCKS as a group policy, and it must be supported in unison by all of the group endpoints within the group, even those that reside in the public Internet.

UDP Checksum Dependency on Source IP Address

An IPsec subsystem using UDP within an ESP payload will encounter NAT induced problems. The original IPv4 source address is an input parameter into a receiver's UDP pseudo-header checksum verification, yet that value is lost after the IP header's address translation by a transit NAT gateway. The UDP header checksum is opaque within the encrypted ESP payload. Consequently, the checksum can not be manipulated by the transit NAT gateways. UDP checksum verification needs a mechanism that recovers the original source IPv4 address at the Group Receiver endpoints.

In a transport mode multicast application GSA, the UDP checksum operation requires the origin endpoint's IP address to complete successfully. In IKEv2, this information is exchanged between the endpoints by a NAT-OA payload (NAT original address). See also reference RFC 3947 (see bibliography). A comparable facility shall exist in a GKM protocol payload that defines the multicast application GSA attributes for each Group Speaker.

Cannot Use AH with NAT Gateway

The presence of a NAT gateway makes it impossible to use an Authentication Header, keyed by a group-wide key, to protect the integrity of the IP header for transmissions between members of the cryptographic group.

B.6 Avoidance of NAT Using an IPv6 Over IPv4 Network

A straightforward and standards-based architecture that effectively avoids the GKM protocol interaction with NAT gateways is the IPv6 over IPv4 transition mechanism RFC 2529 (see bibliography). In IPv6 over IPv4 (a.k.a. "6over4"), the underlying IPv4 network is treated as a virtual multicast-capable Local Area Network. The IPv6 traffic tunnels over that IPv4 virtual link layer.

Applying GKM/IPsec in a 6over4 architecture leverages the fact that an administrative domain deploying GKM/IPsec would already be planning to deploy IPv4 multicast router(s). The group's IPv6 multicast routing can execute in parallel to IPv4 multicast routing on that same physical router infrastructure. In particular, IPv6 multicast routers operating with 6over4 mode enabled on their network interfaces replaces the NAT gateways at administrative domain public/private boundaries.

Within the GKM subsystem, all references to IP addresses are IPv6 addresses for all security association endpoints and these addresses do not change over the group's lifetime. This yields a substantial reduction in complexity and error cases over the NAT-based approaches. This reduction in complexity can translate into better security.

Annex D (informative): Bibliography

ETSI TR 102 287: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects".

ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Services and Architectures".

ETSI EN 301 790 (V1.4.1): "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".

IABG final report: ESA project "IP security over satellites". Contract No. 15555/01/NL/US. 2002

IETF Document: www.ietf.org.

IETF RFC 2362: "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification".

IETF RFC 2529: "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels".

IETF RFC 2627: "Key Management for Multicast: Issues and Architectures".

IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".

IETF RFC 2830: "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security".

IETF RFC 3027: "Protocol Complications with the IP Network Address Translator".

IETR RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)".

IETF RFC 3235: "Network Address Translator (NAT)-Friendly Application Design Guidelines".

IETF RFC 3547: "The Group Domain of Interpretation".

IETF RFC 3947: "Negotiation of NAT-Traversal in the IKE2".

IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

IETF RFC 4082: "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction".

IETF RFC4230: "RSVP Security Properties".

IETF RFC 4301: "Security Architecture for the Internet Protocol".

IETF RFC 4302: "IP Authentication Header".

IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

IETF RFC 4326: "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)".

IETF RFC 4359: "The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)".

IETF RFC 4535: "Group Secure Association Key Management Protocol".

draft-cruickshank-ipdvb-sec-req-04.txt: "Security requirements for the Unidirectional Lightweight Encapsulation (ULE)protocol".

draft-ietf-msec-ipsec-extensions-04: "Multicast Extensions to the Security Architecture for the InternetProtocol".

History

Document history		
V1.1.1	January 2007	Publication