

**Integrated Project 26950 : SATSIX****Deliverable 4000 – 2*****Standardisation impact report (Intermediate)*****Contractual Date of Delivery to the CEC: July 07****Actual Date of Delivery to the CEC: December 07****Author(s): M. Mazzella (TAS-F)****Participant(s): TID, TAS-F, TAS-E, UoA, TPZ , STK, UniS, UVA, HSA, HDT****Workpackage: 4000 Standardisation****Est. person months: 8 M/M****Security: P****Nature: R****Version: 1.0****Total number of pages: 40****Abstract:**

The purpose of the present document is to describe the contribution to the standardisation bodies performed in the frame of the IST- SATSIX project. A copy of the standardisation plan elaborated at the beginning of the project is included. Contribution and participation to the standardisation meetings are mentioned and described.

Finally, conclusions of the IST-SATSIX standardisation activities impact are drawn.

**Keyword list:** Satellite, Broadband, Standardisation, IPv6, ETSI, BSM, IETF

## Executive Summary

The purpose of the present document is to describe the standardisation activities performed in the frame of the **IST- SATSIX** Project. The **IST- SATSIX** project has developed from the beginning a clear standardisation strategy that has been implemented and led to standardisation contribution towards the ETSI - BSM and IETF bodies.

After a short introduction to the **IST- SATSIX** project, the original plan of the standardisation strategy is described (Chapter 3). The strategy described covers the different potential standardisation bodies that could receive **IST- SATSIX** results. The following bodies were envisaged from the beginning: ETSI, and IETF.

The second section (Chapter 4) of the document is related to the impact of the current and emerging standards on the project. There, a list of the main standards that have been relevant for the design and the implementation of the IPv6 into satellite system are presented.

Due to the importance of the standardisation activity in the **IST- SATSIX** project, a dedicated section has been created covering the impact of the **IST- SATSIX** project on the standardisation bodies (Chapter 5). In this section all information related to the different contributions towards the IETF and the ETSI standardisation bodies have been gathered.

Finally, the document concludes with chapter 6.

## **COPYRIGHT**

© Copyright 2006 The SATSIX Consortium

consisting of :

- § Thales Alenia Space (TAS-F), France
- § CNRS/LAAS (LAAS), France
- § University of Rome (UoR), Italy
- § SINTEF (STI), Norway
- § University of Surrey (UNIS), United Kingdom
- § University of Aberdeen (UoA), United Kingdom
- § Telefonica I+D (TID), Spain
- § Thales Alenia Space Espana (TAS-E), Spain
- § B2i (B2i), France
- § Systemtek (STK), United Kingdom
- § Hispasat SA (HSA), Spain
- § University of Valladolid (UVA), Spain
- § Hungaro Digital Plc (HDT), Hungary
- § Telespazio (Italy)

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the SATSIX Consortium. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

All rights reserved.

## DOCUMENT AUTHORS

This document has been generated from contributions coming from most of the SATSIX partners. The contributors are the following:

<b>Partners company</b>	<b>Contributors</b>
<b>TAS-F</b>	Pierre Loyer, Michel Mazzella, Cédric Baudoin
<b>TAS-E</b>	Ana Yung, Elisa Callejo
<b>STK</b>	Robert Mort
<b>UoA</b>	Gorry Fairhurst, Arjuna Sathiaselan, Gerrit Renker
<b>UniS</b>	Haitham Cruickshank

## Table of Contents

1	Introduction.....	1
1.1	Scope.....	1
1.2	Related documents.....	1
1.3	Terminology and definition.....	1
1.4	Abbreviations .....	2
2	Project description .....	4
3	Standardisation activities planning .....	5
3.1	ETSI BSM.....	5
3.2	IETF.....	6
3.3	DVB-RCS/SatLabs.....	6
4	Impact of current or emerging standards on project’ s Work.....	7
4.1	ETSI BSM.....	7
4.2	IETF.....	8
4.3	SATLABS.....	9
5	Standardisation activities performed.....	10
5.1	ETSI BSM Activities.....	10
5.1.1	Introduction .....	10
5.1.2	Impact of SATSIX on ETSI BSM Standards.....	10
5.1.3	Address Management at SI-SAP .....	11
5.1.4	Multicast Source Management .....	12
5.1.5	QoS Functional Architecture.....	17
5.1.6	Inter-working with IntServ QoS .....	20
5.1.7	Inter-working with DiffServ QoS .....	21
5.1.8	General Security Architecture .....	22
5.2	IETF Working Group Documents .....	31
5.2.1	Impact of SATSIX on IETF Standards.....	32
5.2.2	Link-Layer Protocols .....	32
5.2.3	Transport Protocols.....	33
5.3	DVB-RCS Technical Module Working Group .....	34
	Conclusions.....	35
6	References.....	35

## 1 INTRODUCTION

### 1.1 Scope

The scope of this document is to provide a clear overview of the efforts the **SATSIX** Consortium has performed in standardisation of its findings. By participating in standardisation activities, the SATSIX consortium has contribute to the promotion of the IPv6 in particular and of Broadband Satellite Systems in general.

### 1.2 Related documents

<b>RD1</b>	SATSIX Annex 1 : Description of the work
<b>RD2</b>	SATSIX D1000-1: Corporate applications scenario
<b>RD3</b>	SATSIX D1000-2: Residential applications scenario
<b>RD4</b>	SATSIX D1000-3: Collective applications scenario
<b>RD5</b>	SATSIX D1000-4: Satellite Network requirements
<b>RD6</b>	SATSIX D2000-1: Network architecture
<b>RD7</b>	SatLabs System Recommendations. Part 2 – QoS Specifications, v2.0d4 ; September 2006
<b>RD8</b>	ETSI EN 301 790 v1.4.1. Digital Video Broadcasting (DVB); Interaction channel for satellite distribution system; September 2005
<b>RD9</b>	ETSI EN 300 421. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 Ghz satellite services; August 1998
<b>RD10</b>	ETSI EN 302 307 V1.1.1. Digital Video Broadcasting (DVB), Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; March 2005
<b>RD11</b>	ETSI TR 101 790 v1.3.1. Digital Video Broadcasting (DVB); Interaction channel for satellite Distribution Systems; Guidelines for the use of EN 301 790; September 2006
<b>RD12</b>	ETSI TS 102 429-2 V1.1. Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Regenerative Satellite Mesh – B (RSM-B); DVB-S/ DVB-RCS family for regenerative satellites;Part 2: Satellite Link Control layer. October 2006.
<b>RD13</b>	ETSI TS 102 429-3 V1.1. Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Regenerative Satellite Mesh – B (RSM-B); DVB-S/ DVB-RCS family for regenerative satellites;Part 3: Connection control protocol. October 2006.
<b>RD14</b>	ETSI TS 102 293 v1.1.1. Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; IP Interworking over satellite; Multicast group management; IGMP adaptation; February 2004

### 1.3 Terminology and definition

<b>Connection Control Protocol (C2P)</b>	Protocol that provides the interaction between RCSTs and NCC to support set-up, modification and release of
--	---

	connections and channel bandwidth modification.
<b>Control plane</b>	The control plane has a layered structure and performs the connection control functions; it deals with the signalling necessary to set up, supervise and release connections.
<b>DCCP</b>	Datagram Congestion Control Protocol. A new IETF-maintained transport protocol for audio, video and other multimedia data.
<b>Digital Video Broadcasting Return Channel by Satellite (DVB-RCS):</b>	Protocol for an interaction (or return) channel in satellite links.
<b>Digital Video Broadcasting via Satellite (DVB-S):</b>	Protocol for broadcasting TV signals and by extension data over satellite.
<b>Multicast</b>	Communication capability, which denotes unidirectional distribution from a single source access point to a number of specified destination, access points.
<b>Quality of Service (QoS)</b>	Measure of the parameters of a network that influence perceived quality of communications, including the delay, jitter, bandwidth, and packet loss that packets sent by the application experience when being transferred by the network.
<b>UDP-Lite</b>	An IETF-maintained transport protocol for wireless links.

#### 1.4 Abbreviations

<b>ACM</b>	Adaptive Coding and Modulation	<b>MTU</b>	Maximum Transmission Unit
<b>ATM</b>	Asynchronous Transfer Mode	<b>NCC</b>	Network Control Center
<b>BSM</b>	Broadcast Satellite for Multimedia	<b>NRT</b>	Non Real Time
<b>C2P</b>	Connection Control Protocol	<b>OBO</b>	Output Back Off
<b>CAC</b>	Connection Acceptance Control	<b>OBP</b>	On Board Processor
<b>Cnx</b>	Connection	<b>PEP</b>	Performance Enhancement Proxy
<b>COS</b>	Class Of Service	<b>PHB</b>	Per Hop Behaviour
<b>DAMA</b>	Demand Assigned Multiple Access	<b>QoS</b>	Quality of Service
<b>DiffServ</b>	Differentiated Services	<b>RBDC</b>	Rate Based Dynamic Capacity
<b>DCCP</b>	Datagram Congestion Control Protocol	<b>RCST</b>	Return Channel Satellite Terminal
<b>DRA</b>	Dynamic Rate Adaptation	<b>ROHC</b>	Robust Header Compression

<b>DS</b>	DiffServ	<b>RRM</b>	Radio Resource Management
<b>DVB</b>	Digital Video Broadcast	<b>RSGW</b>	Regenerative Satellite Gateway
<b>DVB-RCS</b>	Digital Video Broadcast-Return Channel Signalling	<b>RT</b>	Real Time
<b>DVB-S</b>	Digital Video Broadcasting – Satellite	<b>SCT</b>	Superframe Composition Table
<b>DVB-S2</b>	Digital Video Broadcasting – Satellite Second generation	<b>SNIR</b>	signal to noise and interference ratio
<b>ETSI</b>	European Telecommunications Standards Institute	<b>SNR</b>	Signal to Noise Ratio
<b>FCA</b>	Free Capacity Assignment	<b>SSPA</b>	Solid State Power Amplifier
<b>FCT</b>	Frame Composition Table	<b>ST</b>	Satellite Terminal (BSM)
<b>GSE</b>	Generic Stream Encapsulation		
<b>HPA</b>	High Power Amplifier	<b>TBTP</b>	Terminal Burst Time Plan
<b>IGMP</b>	Internet Group Membership Protocol	<b>TCT</b>	Time slot Composition Table
<b>IP</b>	Internet Protocol	<b>TDM</b>	Time Division Multiplexing
<b>IPv4</b>	IP version 4	<b>TFRC</b>	TCP-Friendly Rate Control
<b>IPv6</b>	IP version 6	<b>TSGW</b>	Transparent Gateway
<b>MAC</b>	Media Access Control	<b>TWTA</b>	Travelling Wave Tube Amplifier
<b>MDP</b>	Markov Decision Process	<b>ULE</b>	Unidirectional Lightweight Encapsulation
<b>MLD</b>	Multicast Listener Discovery	<b>VBDC</b>	Volume Based Dynamic Capacity
<b>MMT</b>	Multicast Map Table	<b>VCI</b>	Virtual Channel Identifier
<b>MRC</b>	Model Reference Control	<b>VPI</b>	Virtual Path Identifier

## 2 PROJECT DESCRIPTION

The main objectives of SATSIX are :

- to lower the cost of broadband satellite access, through the development of new satellite access techniques and the integration of wireless local loops (WiFi and WiMax);
- to develop recommendations, testbeds, trial networks showing how satellite broadband access shall integrate Next Generation Networks, based on IPv6, and support new multimedia applications.

The SATSIX project will thus focus on satellite systems that offer attractive solutions to the access segment of wider networks in several main scenarios, that allow:

1. for all types of users, to access the Internet and other widely distributed networks (e.g. Virtual Private networks - VPN's) directly or via local networks (WiFi or WiMax, LAN etc.)
2. for corporate and SME users, to set up (virtual) private networks via a backbone including satellite systems inter-working with terrestrial networks where necessary.

The project aims at demonstrating that satellite systems can be very good drivers for the deployment of IPv6 in the Internet, and could even play a key role. They can offer a cost effective and rapid solution for ISP's to provide native IPv6 connectivity and services to geographically spread early interested users.

### 3 STANDARDISATION ACTIVITIES PLANNING

The SATSIX consortium has planned during the duration of the project to actively participate to the relevant standardisation activities. The SATSIX project will constantly monitor current and emerging standards activities to ensure that its work is taken into account in, and is consistent with, the latest standards. The standards or recommendations concerned notably include those generated by ETSI, IETF, DVB and SatLabs.. This section reflects the standardisation plan as described at the beginning of the project.

#### 3.1 ETSI BSM

Current work aims to produce specifications that extend the scope of Broadband Satellite Multimedia (BSM) standards. The BSM architecture and related concepts are designed as the basis of an open platform based on IP service delivery. However, more work is urgently needed to further develop and extend the standards for IP inter-working functions and related network services that have already been identified, both within ETSI and in other standards bodies.

Satellite networking standards are needed to promote the convergence of satellite access network services with the established and emerging terrestrial access services by providing a comprehensive framework for standards-based inter-working between satellite networks and terrestrial IP networks (both Intranets and Internet).

SATSIX will be represented in ETSI BSM by expert partners (TASF, TASE, STK, UoA, UniS). It is expected that the project will significantly contribute to the following continuing BSM topics:

- DVB/RCS Connection Control Protocol (C2P) requirements
- GSE-protocol-spec-v09, IP/S.2 study of DVB-GBS, Document rev 9 was approved by the DVB-TM in March 2007. The corresponding blue book (GBS-0436r10) was issued in May (Digital Video Broadcasting (DVB);Generic Stream Encapsulation (GSE) Protocol and support). Support will continue (as required) until published by ETSI in 2007
- Development and refinement of BSM specifications for the SI-SAP.
- Refinement of the security BSM security architectures (unicast and multicast).

Mesh DVB-RCS/DVB-S satellites networks strength is to provide direct connectivity (only one satellite hop) between sites. Mesh IP communications enable the possibility of carrying traffic LAN-to-LAN, secure communications without a Hub involved, Intranet, and two-way traffic generated by real time applications (e.g. videoconferencing, VoIP). But as already demonstrated from the first Mesh DVB-RCS/DVB-S regenerative system demonstrator during FP5 IBIS project, it requires a Connection Control Protocol (C2P).

C2P is capable of setting up MAC connections to convey any traffic transmission among RCSTs. It enables a dynamic connection control interface between the NCC and RCSTs. But even more, C2P may not only solve the mesh problem, it also brings extra flexibility and efficiency to DVB-RCS systems, in terms of dynamic bandwidth and dynamic resource allocation.

The first C2P initiative was identified in the frame of the DVB-RCS technical activities in 2001. It was accepted by the DVB-RCS group and included as Annex J of DVB-RCS Guidelines. Alcatel Alenia Space España, now Thales Alenia Space España, completed this proposal in 2004 based on their experience with AmerHis System ESA ARTES3 project, the first multi-beam DVB-RCS/DVB-S regenerative satellite system, capable to provide simultaneous star and mesh communications. At this time, a new element entered the discussion, i.e. the possibility of having peer-to-peer communications using the DVB-RCS standard. The C2P applied for a regenerative scenario could also be applied to a mesh transparent scenario. Finally, Annex J in the DVB-RCS Guidelines was updated to constitute the

basic elements of the C2P, a first step for the protocol implementation. The full specification of the protocol, to be applicable to any DVB-RCS system, whether transparent or regenerative, star or mesh, single-beam or multi-beam was left out for coming activities.

In parallel, Telecommunications Industry Association (TIA) started to work on a C2P standard for Satellite Network Mode Systems (SNMS). A draft named SMCP (SNMS Mesh Control Protocol) was prepared by TIA WG 34.1 and it arise elements that could not be DVB-RCS compliant.

It was then decided to perform a C2P development within ETSI TC SES (Satellite Equipment and Systems) in order to link and combine all C2P activities. ETSI SES BSM created two work items: a general C2P standard and a C2P for DVB-RCS systems, both approved with the support from ESA-SatLabs, DVB-RCS, Telecommunications Industry Association (TIA) and ETSI SES BSM. These two work items were created in order to link and combine all C2P activities. TAS-E has been the responsible for the coordination and liason between all the different groups.

### **3.2 IETF**

Currently the ipdvb (IP over DVB) Working Group (WG) is active in satellite-specific areas concerning several aspects of IP over DVB transport. Within this WG the project, through specific expert partners (especially UoA and UniS), will contribute to layer 2 encapsulation, ARP and security.

In addition, other WG's of special relevance to satellite issues will be supported by the project, notably msec WG (Multicast Security) , concerning multicast security. The project will generate Internet Drafts for the above WG's and contribute to the WG's work. The project will also consider contributing to the rohc WG (Robust Header Compression), should this group start activities that are appropriate to DVB technologies.

It is therefore expected that the project will significantly contribute to the following topics:

- § Header Extension formats for GSE & ULE, IETF IPDVB WG, draft-fairhurst-ipdvb-ule-ext-xx.txt. Chartered to be submitted in: Aug 2007. Publication expected April 2008.
- § UDPLite-MIB, IETF TSV WG, draft-renker-tsvwg-udplite-mib-xx.txt. Publication expected April 2008.
- § Faster restart, IETF DCCP WG, draft-ietf-dccp-tfrc-faster-restart-xx Target date for review: Dec 2007. Publication expected June 2008
- § Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol in the ipdvb working group: draft-ietf-ipdvb-sec-req-xx.txt. Publication expected April 2008.
- § Multicast IP Security Composite Cryptographic Groups in the msec working group: draft-ietf-msec-ipsec-composite-group-xx. Target date for publication: Oct 2007.

### **3.3 DVB-RCS/SatLabs**

Compliance to DVB-RCS is more and more a differentiating factor on the market. Previously, customers were simply requesting a DVB-RCS solution but now customers request a DVB-RCS certificate to prove compliance. The DVB-RCS community (operators, manufacturers, space agencies), grouped in the SatLabs organisation (now an European Economic Interest Grouping - EEIG), is committed to ensuring interoperability among DVB-RCS terminals and systems and the availability of solutions for interoperability testing and certification. SatLabs has therefore developed a test bed and selected a laboratory that will conduct Terminal certification testing (operational by April 2005).

SatLabs, initiated by the European Space Agency, has the support of a wide representation of industry. It should be noted that SatLabs aims to define a subset, or set(s) of common options of DVB-RCS and of implementation aspects that should simplify the production and reduce the cost of equipment. SatLabs is also a major contributor to DVB-RCS standard evolutions. However SatLabs has no funding to develop or demonstrate solutions, and these aspects are left to industry. This offers an opportunity for SATSIX to make an important contribution in terms of validation and demonstration of the SatLabs recommendations.

The SatLabs Group is an international, not-for-profit association whose members are committed to bringing the deployment of the DVB-RCS standard to large-scale adoption.

SatLabs membership is comprised of service providers, satellite operators, system integrators, terminal manufacturers and technology providers with an interest in DVB-RCS. The main goal of the SatLabs Group is to ensure interoperability between DVB-RCS terminals and systems and to achieve low-cost solutions. The SatLabs Qualification Program was launched in April 2005 to achieve this goal by providing an independent certification process. When a terminal has successfully passed the tests defined in the SatLabs Qualification Program, a Certificate of Compliance is granted and the terminal is defined as a "Verified Product".

The SATSIX project will contribute to SatLabs informally through common partners in establishing consensus, and also directly using project results when appropriate and depending on the agenda of SatLabs. It is expected that the project will contribute through participating partners (TASE, TASF, HSA) to the following topics which are being actively discussed:

- § Security
- § QoS & Radio Resource Management.
- § Connection Control Protocol

but also to future topics that SatLabs may have to address such as:

- § IPv6 support
- § WLL – satellite link inter-working
- § Optimised encapsulation and header compression support.

SATSIX will be represented SatLabs meetings by expert partners (TASF, TASE).

Contributions are expected in order to help the specification of IPv6 support, improvements on GSE&ULE encapsulation methods that can improve the efficiency of DVB-RCS systems and the liaison between ETSI SES BSM and SatLabs working groups.

## **4 IMPACT OF CURRENT OR EMERGING STANDARDS ON PROJECT' S WORK**

### **4.1 ETSI BSM**

AmerHis systems does represent the first DVB-RCS/DVB-S multi-beam regenerative system that implements C2P for simultaneous star and mesh connectivity. Therefore the experience won with AmerHis plus the new studies done in the frame of SatSix project are representing a considerable contribution for the finalization of the C2P standardization.

The full specification of the protocol is to be applicable to any DVB-RCS system, whether transparent or regenerative, star or mesh, single-beam or multi-beam.

The ETSI C2P TR 102 603 High Level Design and Guidelines, has been approved by SES BSM group last 11<sup>th</sup> of December. The protocol specification, ETSI C2P TS 102 602 Connection Control Protocol (C2P) for DVB-RCS will be approved during the first quarter of 2008. The new DVB-RCS coming version v1.5.1, will be updated also taking into account the impact of C2P and mesh networking.

Monitoring the of standardisation tracking:

- Ü Address Management at SI-SAP (satellite-independent service access point)
- Ü Multicast Source Management
- Ü QoS Functional Architecture
- Ü Interworking with IntServ QoS
- Ü Interworking with DiffServ QoS
- Ü General Security Architecture
- Ü Multicast Security Architecture
- Ü Transition to IPv6.
- Ü DVB-RCS C2P (connection control protocol) requirements (on-going work).

SATSIX has also used the ETSI BSM specifications as a basis for its system designs. SATSIX examines and implements specific instances of satellite networks and therefore the ETSI standards have been extrapolated for this purpose, in particular for DVB-RCS implementation.

The BSM protocol architecture used throughout the standards is characterised by a clearly defined boundary at the “SI-SAP” [13] separating the common Satellite-Independent (SI) protocol layers and alternative lower Satellite-Dependent (SD) layers. This concept has enabled the BSM WG to address complex technical issues in a systematic and consistent manner. This interface has also enabled treatment of issues for the IP layer and above for all types of satellite system and independently of the satellite technology-specific layers below the interface.

As a result of this approach and also due to the wide industry participation and consensus in the BSM WG, the results are intended to have generic application for IP services to different satellite systems.

Therefore for SATSIX, it is mainly the functionalities from IP-layer and above which have been extracted and used as a basis for the specific examples and features defined in the further detail. These relationships are illustrated in detail in the SATSIX deliverables.

Another important activity concerns the definition of the GSE protocol, either concerning the encapsulation itself or the way to use it in satellite systems (signalisation issues, coexistence or transition with MPEG2-TS, ...). This encapsulation scheme will improve the overall efficiency and make easier the convergence with other IP based networks. This work is now discussed in other DVB groups, such as TM-T2, in order to define an encapsulation scheme applicable to all DVB networks (same level as MPE).

## 4.2 IETF

Monitoring the standardisation tracking work relating to new generation transport protocols for multimedia applications. This work is feeding simulation activities in WP2500 and development of exemplar applications and protocol stacks for WP3000. Specific contributions have been made on security extensions for DVB (via the ipdvb WG), support for signalling at L2 for GSE (via the ipdvb WG), support for radio links (via TSVWG), and evolution of new mechanisms able to accommodate the variety of path characteristics experienced in DVB networks (dcp WG). In all these activities, work has spanned fundamental analysis of the problem within related SATSIX work packages, production of Internet Drafts and contributions to the appropriate Working Groups. This has to drafting of the final documents, and is expected to result in final acceptance of the documents as published RFCs by the end of the SATSIX Project (or shortly thereafter).

The contribution on extension mechanisms for ULE has also formed a normative part of the DVB GSE specification, which has been approved for publication as an ETSI TS.

### 4.3 SATLABS

As a first step, SatLabs has accomplished the specification for test certification for a star transparent DVB-RCS system. TAS-E main contribution to the group has been based on the extension of the specification to any DVB-RCS system, looking for the harmonization of the management and control plane of any DVB-RCS system.

In the frame of SatLabs, TAS-E has published a white paper based on AmerHis / Satlife experience.

Ana Yun, Josep Prat, “AmerHis: DVB-RCS meets mesh connectivity”

White papers accessible via <http://satlabs.org/content/view/87/79/>

TAS-E has also represented the official liaison between ETSI SES BSM and SatLabs group, with the responsibility of coordination between the two groups.

SatSix project interest in SatLabs is to be up to date in what is now required to be SatLabs certification, getting the first feedback from DVB-RCS terminals and Hubs manufacturers, operators and technology providers of what are the technology trends for the coming years, in order to move SatSix results closer to the market.

A strong activity was also followed for C2P, the Connection Control Protocol for DVB-RCS systems. For this purpose TAS-E has being the rapporteur and coordinator between the different standardization groups and actors involved in the C2P activity: TIA, ETSI, TM-RCS and ESA-SatLabs.

## 5 STANDARDISATION ACTIVITIES PERFORMED

This section contains a summary of the different standardisation related activities performed by the SATSIX consortium. A list of the contribution and relevant document is included in the section.

### 5.1 ETSI BSM Activities

#### 5.1.1 Introduction

The ETSI BSM (Broadband Satellite Multimedia) WG focuses on IP-based networks and the associated needs for standardisation when satellites are integrated within them.

The BSM group comprises major organisations from the satellite world and therefore its outputs represent a consensus of the most important techniques and solutions relevant in this sphere of activity. SATSIX has had an important influence on the standards produced through the many contributions made and resulting technical discussions.

The most recent phase of work of the ETSI BSM WG starting in 2005 has resulted in specifications for generic broadband satellite systems aimed at supporting optimal IP-based services integrated within Next Generation Networks. The existence of a set of relevant open standards is intended to enable service providers to identify and support common service platforms, and manufacturers to design competitive solutions.

The main subjects addressed are as follows:

- Address Management at SI-SAP (satellite-independent service access point)
- Multicast Source Management
- QoS Functional Architecture
- Interworking with IntServ QoS
- Interworking with DiffServ QoS
- General Security Architecture
- Multicast Security Architecture
- Transition to IPv6.
- DVB-RCS C2P (connection control protocol) requirements (on-going work).

The standards resulting from the completed work items can be freely accessed on the ETSI site: [portal.etsi.org](http://portal.etsi.org).

The sections below give outlines of the ETSI specifications generated. The full details are available in the references given.

#### 5.1.2 Impact of SATSIX on ETSI BSM Standards

The ETSI BSM work has been actively supported by inputs from SATSIX partners, and it can be fairly stated that the recent BSM standards have depended to a great extent on SATSIX partner involvement. This is due to the fact that SATSIX partners have acted, or are still acting, as rapporteurs for several of the standards, namely:

Standard	Rapporteur
Address Management at SI-SAP (satellite-independent service access point)	STK
Multicast Source Management	STK
QoS Functional Architecture	STK

Interworking with IntServ QoS	<b>STK</b>
General Security Architecture	<b>UNIS</b>
Multicast Security Architecture	<b>UNIS</b>
DVB-RCS C2P (connection control protocol) requirements.	<b>TAS-E</b>

The nature of ETSI BSM standards, being generic in terms of satellite technology and independent of whether DVB (-RCS) etc. is used as the data link layer, means that SATSIX solutions at the lower layers have not been directly used in the standards, apart from as examples. Nevertheless SATSIX concepts at the generic IP layer (and above) have been used to influence the standards.

### 5.1.3 Address Management at SI-SAP

This subject [14] describes the relationships between IP addresses and lower layer addresses, called BSM\_IDs as a generic term for lower layer addresses in different satellite systems (for example in a DVB-RCS system the BSM\_ID could relate to a MAC address). It also covers how to create, manage, and query the BSM\_IDs for the purpose of sending and receiving user data (in particular IP packets) via the SI-SAP.

The task divides into two parts:

1. address management scenarios and architectures,
2. unicast address resolution at the SI-SAP,

The technical standard document elaborates the details of the address management functions, notably the address resolution function for relating BSM\_IDs to IP addresses.

BSM Address Resolution (B-AR) is defined as the function that associates a BSM\_ID with the corresponding IP Address. The BSM Architecture (see Figure 1) must provide a service where AR is supported for B-AR clients in all STs by a central B-AR server. In this content, STs includes both the Gateways (typically the Hub for a Star network) and remote STs. Each ST should also have an AR table as part of the B-AR client.

The B-AR server could, in principle, be located anywhere but it is realistic to assume that is under the control of the BSM operator since it needs knowledge of the BSM address space. Typically, the B-AR Server will be located at a Gateway or at the NCC. Having the B-AR server located at the NCC may be appropriate if the AR function is used to support traffic management, i.e. allowing and denying IP packets access to the BSM network.

B-AR is a C-plane function. However, two distinct processes are required for AR to function. Above the SI-SAP, a BSM\_ID must be associated with an IP address. Below the SI-SAP, a BSM\_ID is associated with a MAC address. The BSM\_ID must be resolved to a MAC address whenever an IP packet has to be transmitted by the lower layers; this is also usually a static or pseudo static process. The process of association can store pairs of values in a table, as is the case with entities using AR over wired networks such as Ethernet. The process of resolution can examine the table, usually stored at the location where resolution occurs. Mechanisms are required to populate and update the local tables that store the associations. Updates to a local table will normally be performed by periodically transferring data from a central, or reference, table. The transferred data will either replace or enhance local data. It is highly desirable to minimise the flow of B-AR data traversing the satellite link.

B-AR may be used whenever an IP packet is to be forwarded to a new destination across a BSM network. The BSM\_ID of the next hop must be determined for the packet to be forwarded, and B-AR must be used if the BSM\_ID for a given next hop IP address is not already known at that ST. There are three cases:

1. star network inbound: all IP addresses resolve to the hub gateway BSM\_ID. The BSM\_ID associated with the hub gateway is either acquired at ST startup as part of Configuration Management by the NCC or it is pre-programmed,
2. star network outbound: IP addresses resolve to specific BSM\_IDs. IP address resolution may require policy decisions in connection with access management. An OBP Satellite that performs layer 2 switching may need an AR table that is at least partially managed by the B-AR server,
3. mesh network: IP addresses resolve to specific BSM\_IDs. IP address resolution may require policy decisions. An OBP Satellite that performs layer 2 switching may manage an AR table itself or it may be managed by the B-AR server.

In all cases a B-AR client at the sending side performs address resolution. In the first instance this should use the cached entries in the local AR table, but if there is no match the ST sends an address resolution request to a B-AR server whose address is acquired dynamically or is pre-configured.

NOTE: In contrast to Ethernet ARP a B-AR client should never send a broadcast message over the satellite link (this may not be possible in any case) and should use the address of the known B-AR server.

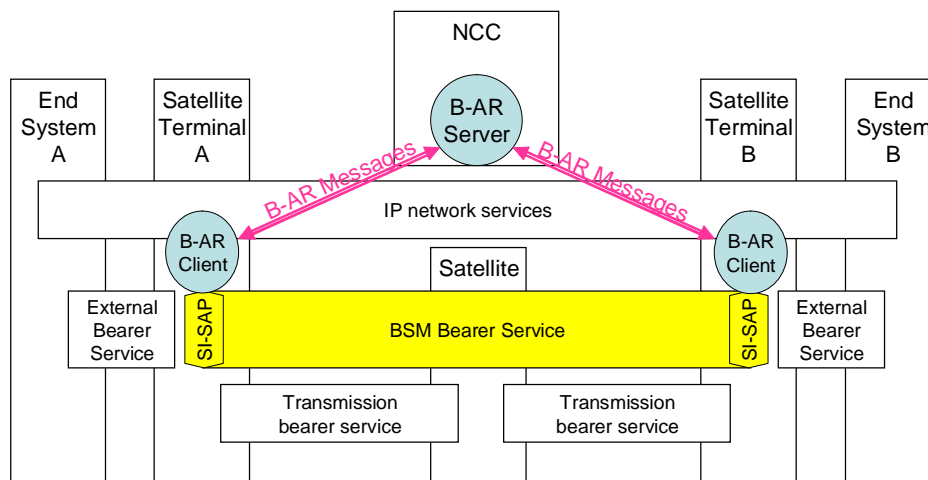


Figure 1: BSM AR Architecture

#### 5.1.4 Multicast Source Management

This subject [15] defines the architectures and functions required for the interworking of IPv4 multicast protocols, including multicast sources, with the BSM.

The technical standard document firstly considers the BSM network scenarios for IP multicast interworking, including two main aspects:

1. the satellite network architecture
2. management of multicast sources and data forwarding, either statically or dynamically.

The BSM functional and protocol architectures are then derived for management of:

- IP multicast control messages (group management and routing protocols),
- Multicast access control (including resource management) and
- Multicast address resolution.

The document then defines the detailed functional requirements and interactions of the above three functions with respect to the BSM lower layer interface, the SISAP. The Satellite-Dependent (SD) functions below this interface are system specific and are not treated here.

In the case of multicast routing protocols, the PIM-SM protocol (including the PIM-SSM variant) is taken as the basis for this document since it is almost exclusively used in existing and proposed multicast routing applications today.

IPv6 protocols are not explicitly covered here, though they may be compatible with the architectures described.

To make multicast services effective over the BSM, multicast must take advantage of satellite's native multicast capabilities. Unlike Unicast, where destination IP and link layer addresses are specific to an end host, multicast employs a common IP "group" address for a given flow to all receivers, and therefore the BSM SISAP should also employ a corresponding common address, or GID (Group ID), for each multicast flow. The way in which these GIDs are controlled and employed is also defined in this document.

The four main network scenarios and their features are summarised in Table 1, where the network configuration is either star or mesh.

star topology - refers to a star arrangement of links between a central Hub station and remote STs through the satellite. The Hub acts as the sole BSM ingress router and distribution node for BSM multicast. The ST's are all egress routers connected either directly to hosts or via premises networks.

mesh topology – refers to a mesh arrangement of links between STs where all ST's can be interconnected directly through the satellite and each ST can act as a multicast distribution node to ST's. ST's can therefore be both ingress and egress routers.

Scenario	Multicast traffic Ingress Point	Multicast traffic Egress Point	BSM network IP multicast control	Ingress IP multicast control	Egress IP multicast control	BSM Access Control	BSM Address Management
STAR PUSH	Hub	ST	None	None/IGMP/PIM	None/IGMP/PIM	Static	Static/Dynamic
STAR PULL	Hub	ST	IGMP/PIM	IGMP/PIM	IGMP/PIM	Dynamic	Dynamic
MESH PUSH	ST	ST	None	None/IGMP/PIM	None/IGMP/PIM	Static	Static/Dynamic
MESH PULL	ST	ST	IGMP/PIM	IGMP/PIM	IGMP/PIM	Dynamic	Dynamic

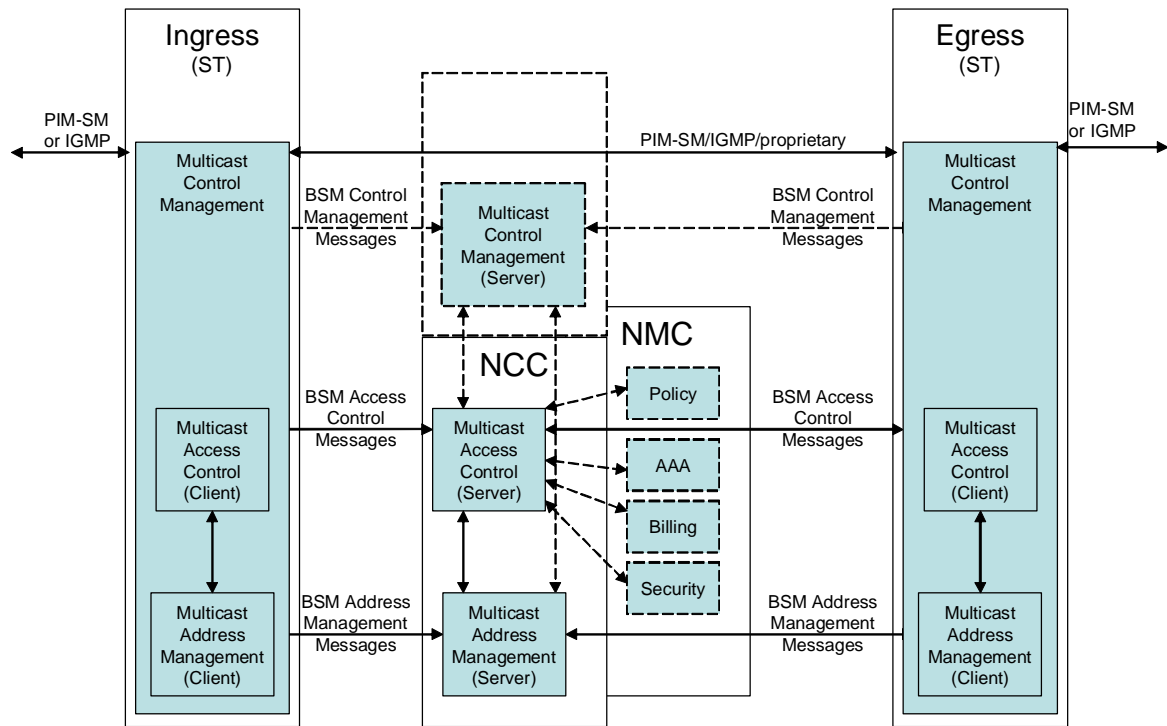
**Table 1: BSM multicast network scenarios**

The above push and pull cases refer to:

push – multicast services are configured by the BSM network operator, or similar centralised management entity, in terms of which groups are forwarded over the BSM on a quasi-static basis. The manager may not always know in advance what kind of resources (bandwidth, delay, jitter) will be required for a given multicast flow, but it has to configure BSM resources based, for example, on a service level agreement.

pull – multicast services are requested and initiated dynamically (i.e. on demand) by each receiver host issuing a "join" to an IP multicast group, and therefore by relay through each egress ST, to the Ingress ST using IP multicast protocols. The conditions under which new group membership can be allowed and the associated multicast flows forwarded over the BSM are determined by BSM network policies.

The Functional Architecture shown in **Figure 2** is an example for the Mesh Pull scenario. This architecture is focussed on the functional entities involved in the end-to-end BSM multicast control mechanisms that enable multicast flows to be forwarded or removed across the BSM from Ingress to Egress. The architecture must support dynamic control of multicast groups, allowing groups to be added and removed on demand.



**Figure 2: BSM Multicast Source Management Control Plane Architecture (Mesh Pull example)**

BSM Multicast Source Management refers to the combination of Control Plane functions needed to create, maintain and remove BSM multicast distribution trees, and which includes Multicast Control Management (using PIM and IGMP), Multicast Access Control, and Multicast Address Management.

The NCC is concerned with BSM SISAP and SD layer functions. The NMC is considered closely related to, or part of, the NCC, whose actions are performed under the aegis of the NMC for aspects such as policy, security and authentication.

**Figure 3** shows the message flows for the Mesh Pull scenario.

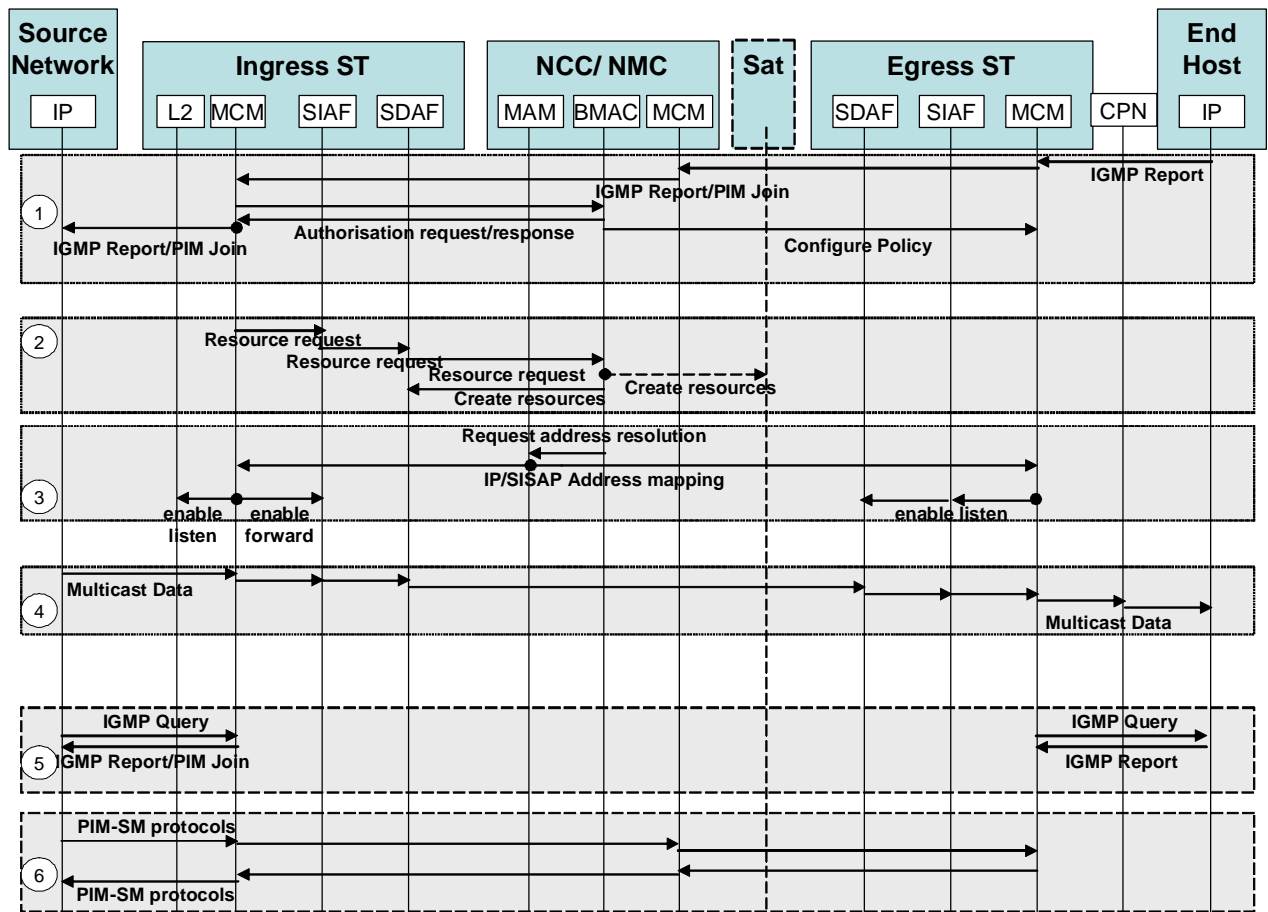
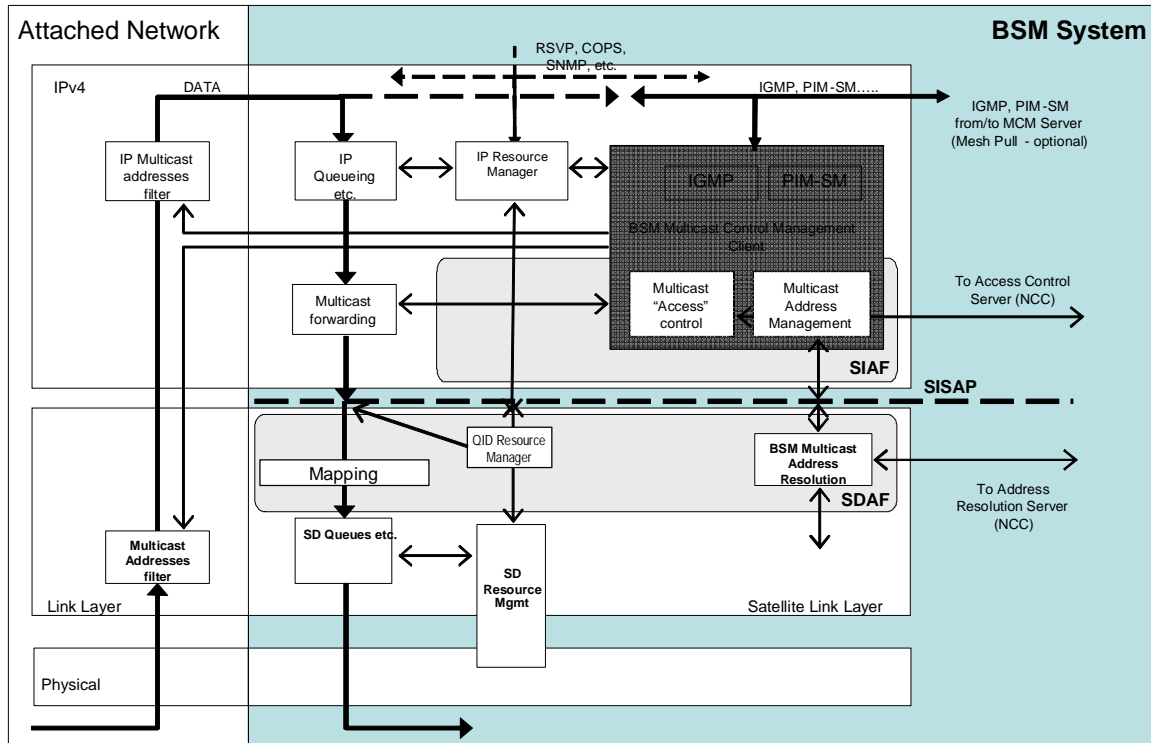


Figure 3 Mesh Pull Scenario Messages

The detailed Multicast Source Management: architecture considers the three constituent functions:

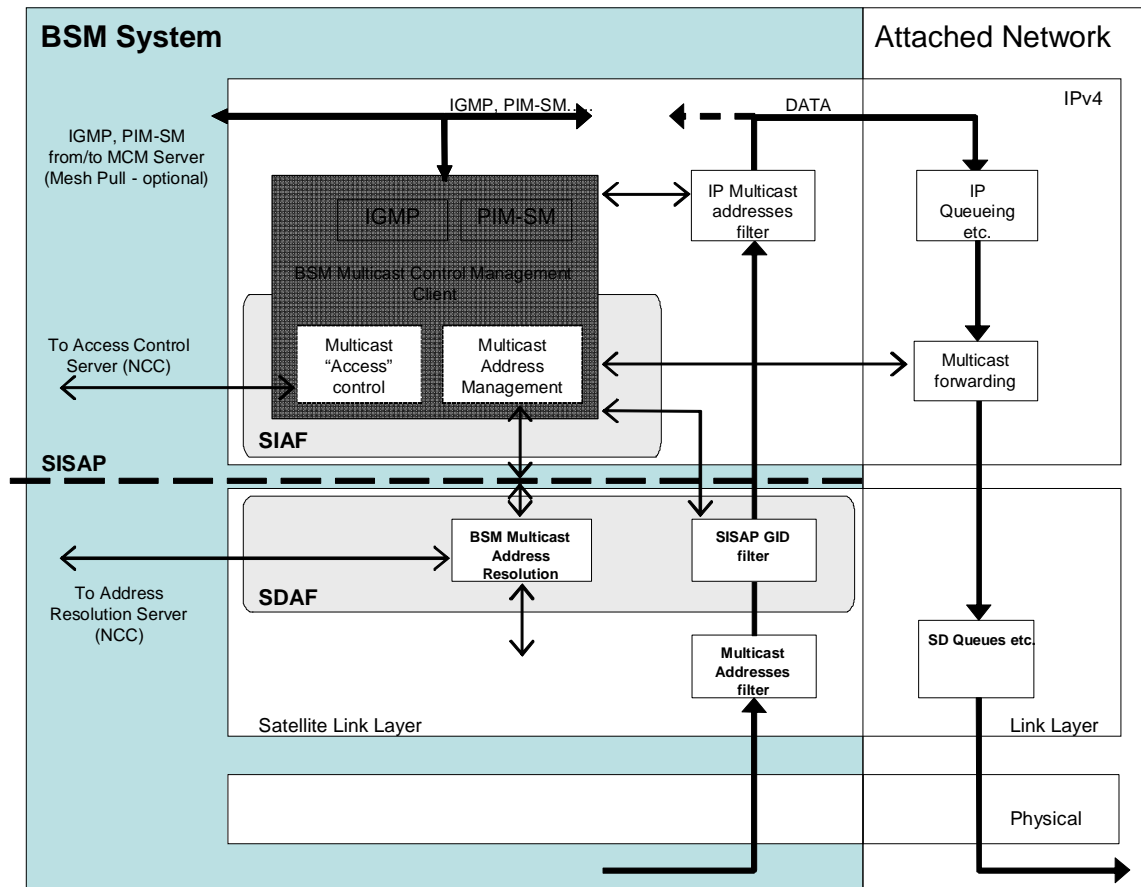
1. Control Management (MCM)
2. Access Control (BMAC)
3. Address Management (MAM).

The protocol architecture differs between the Ingress or Egress ST's, as shown in **Figure 4** and **Figure 5**.



**Figure 4: Detailed BSM Multicast Ingress ST protocol stack**

In the above figure the IGMP/PIM protocol entity (in the MCMC) establishes the IP group membership list (under the aegis of the BMAC) for each of the Ingress ST BSM interfaces. Whenever there is a change of aggregate group membership over all of these interfaces, and/or periodically as necessary, the MCMC sends a resolution request for any new groups to the lower layers of the attached network in order to obtain associated link layer addresses. It also sends a resolution request for the groups to the SISAP to obtain associated GIDs on the BSM side. Reception and forwarding of multicast groups is controlled by the MCMC, and having obtained the BSM resources necessary, the MCMC issues a “Listen” command to the attached network interface together with the binding of relevant IP groups and multicast link layer addresses. The MCMC also issues a “forward” command to the IP forwarding engine together with the binding of the groups to GIDs.



**Figure 5: Detailed BSM Multicast Egress ST protocol stack**

In the above figure the IGMP/PIM protocol entity (in the MCMC) establishes the IP group membership list (under the aegis of the BMAC). Whenever there is a change of group membership it issues a join request to the upstream router.

The MCMC also sends a resolution request for any new groups to the SISAP to obtain associated GIDs on the BSM side. It also sends a resolution request for the groups to the lower layers of the attached network in order to obtain associated link layer addresses. Reception and forwarding of multicast groups is controlled by the MCMC, and it issues a “Listen” command to the IP forwarding engine together with the binding of the groups to GIDs. The MCMC also issues a “forward” command to the attached network interface together with the binding of relevant IP groups and multicast link layer addresses.

### 5.1.5 QoS Functional Architecture

QoS is a network feature which will be increasingly valuable for service differentiation and support of more QoS-sensitive applications. In contrast to wired or optical networks where over-provisioning of capacity is often used to ensure QoS for packet-based transport, satellite systems, as for other wireless networks, allocate capacity efficiently and carefully. This requires more sophisticated QoS methods that are closely linked to resource provision and control at lower protocol layers than IP.

No standardised or common approach to network architecture for end-to-end QoS provision to applications exists at present.

Various approaches to QoS provision can be proposed based on varying complexity and performance. A modular architecture is therefore required which can be adapted to meet different needs.

QoS provision within ETSI BSM systems is one of the first aims, but since BSM systems are intended to access the Internet, end-to-end QoS across integrated networks including satellites is also important.

A BSM QoS functional architecture has been defined for IP-based applications [16]. Compatibility with QoS requirements for generic internetworking including Next Generation Networks (NGN's [22]) are taken into account.

The BSM architecture is characterised by the separation between common Satellite-Independent (SI) protocol layers and alternative lower Satellite-Dependent (SD) layers. At the SI layers, several methods of ensuring end-to-end QoS over integrated networks are foreseen, by means of signalling protocols (e.g. based on SIP) at the session (or application) layers and DiffServ, RSVP/IntServ, or NSIS at the IP layer. At the SD Layers alternative lower protocol layers offer different QoS characteristics. The focus of the architecture definition here is on maintaining compatibility with these alternative methods and approaches by addressing the generic BSM QoS functions required in the SI layers (including IP). These functions will provide interfaces where appropriate with higher-layer and lower-layer QoS functions, and with external networks and customer equipment.

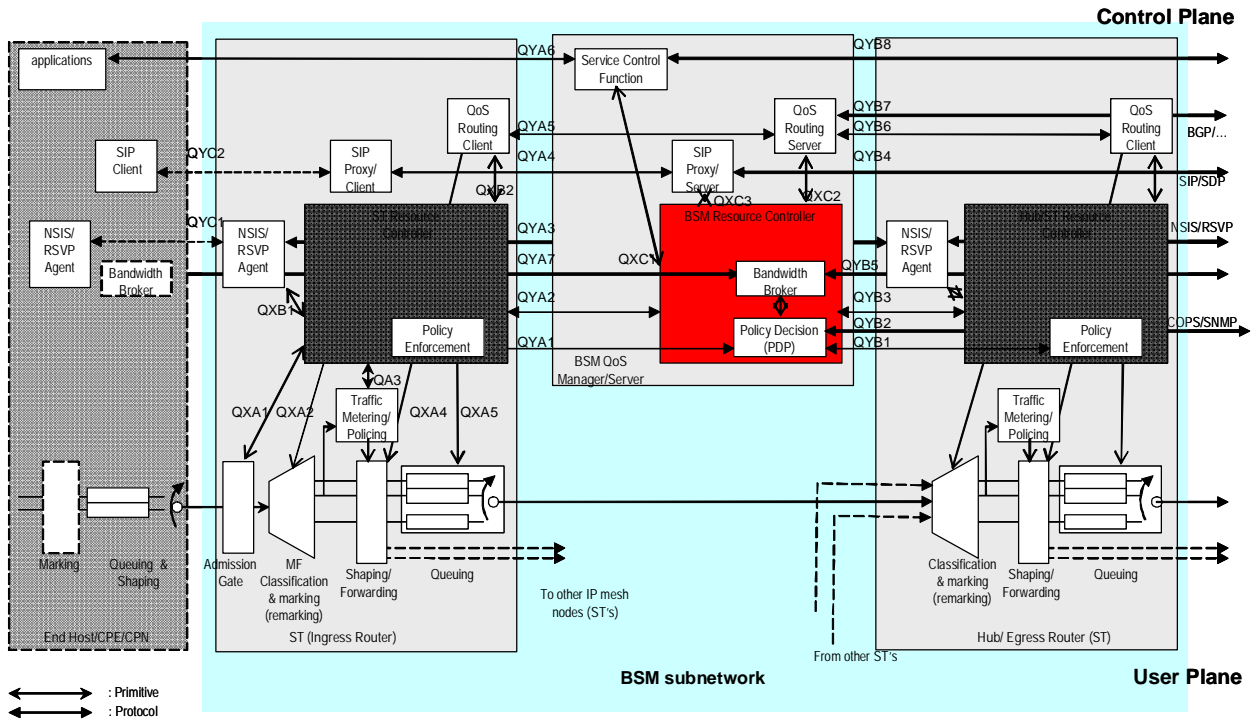
The BSM Global QoS functional architecture, including the relationship of the BSM with QoS protocol layering and with the rest of the network, is illustrated in Figure 6. The figure also shows the range of possible functions involved in QoS and their functional partition between Control and User Planes (Management functions are not shown for clarity since they are more implementation-specific).

Two main kinds of message flows between functional blocks are indicated in the diagram: primitives between protocol layers, and secondly peer-to-peer protocols. Note that the peer-to-peer protocols are shown as horizontal lines for clarity, though in reality they are transported via the user plane.

The BSM QoS architecture is based on centralised control and management of the BSM subnetwork through a Server entity called the BSM QoS Manager (BQM). Like typical servers the BQM can consist of several physical entities. The ST's, as network edge devices, are responsible for traffic processing and policy enforcement at the ingress and egress, but they should be controlled from the BQM. The BQM should contain all the necessary functions to manage QoS for all layers above the SISAP in both Management and Control Planes. The BQM interacts with equivalent local functions in the ST's.

The control and management functions below the SISAP (for connection control, bearer set up, BSM QoS etc.) are usually also centralised in the NCC, which may be closely associated with the BQM.

Many of the functions in the BQM are standardised functions such as those for signalling (RSVP/NSIS or SIP Proxy/SDP), but others specific to the BSM, such as those for managing the BSM's global IP and SIAF layer resources, are allocated to a functional entity called the BSM Resource Controller (BRC).



**Figure 6: BSM QoS Functions in the IP layer and higher layers (one data direction shown)**

Central to the QoS capability of the BSM is the interface of the IP layer with the lower SD layers at the SISAP. To abstract the User Plane QoS interface at the SISAP the concept of QID's (Queue Identifiers) has been introduced. These represent abstract queues available at the SISAP, each with a defined class of service for transfer of IP packets to the SD layers.

The satellite dependent lower layers are responsible for assigning satellite capacity to these abstract queues according to the specified queue properties (e.g. QoS). The QID is not limited to a capacity allocation class; it relates also to forwarding behaviour with defined properties.

A QID is only required for submitting (sending) data via the SISAP and the QID is assigned when the associated queue is opened. An open queue is uniquely identified by the associated QID: in particular, the QID is used to label all subsequent data transfers via that queue.

The way in which QIDs are mapped to the IP layer queues is an important consideration for overall QoS.

The different cases of interaction between QoS requests and the BSM involve not only the User Plane containing the QIDs, but also the Control and Management Planes that influence the way the QIDs are used. The interaction between the IP layer QoS and the SD layer QoS takes place across the SISAP and is thus the major issue for the BSM.

An architecture for the ST ingress is shown in Figure 7.

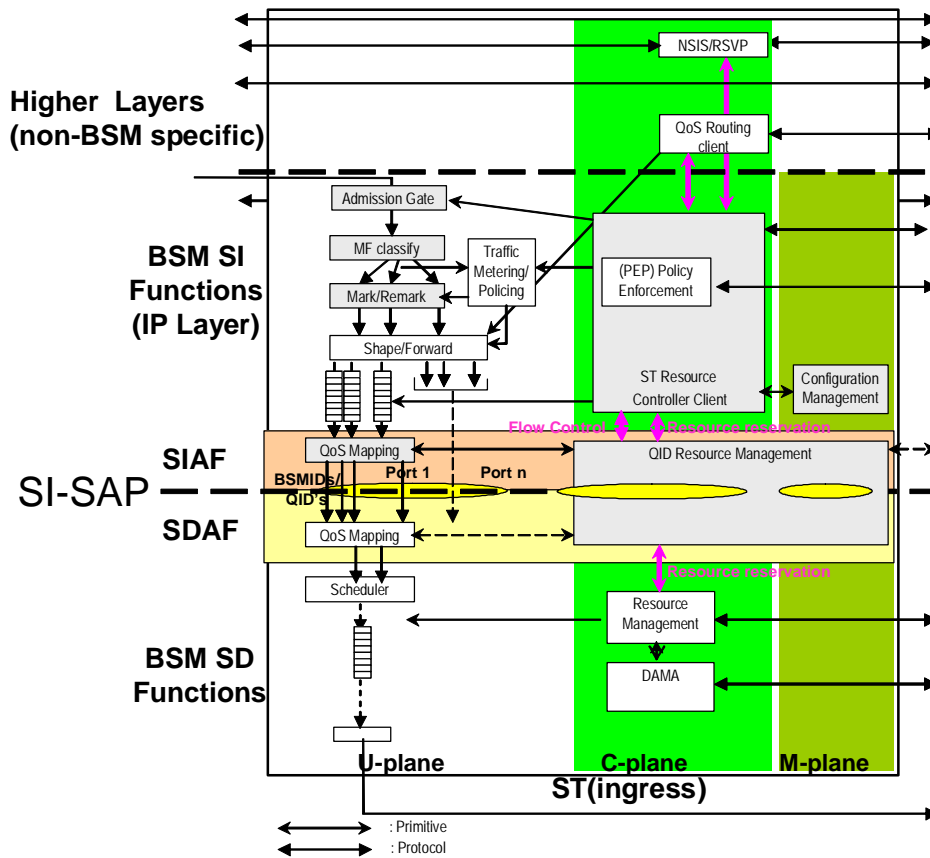


Figure 7: ST ingress architecture across the SISAP

### 5.1.6 Inter-working with IntServ QoS

The key to providing real-time multimedia services such as those offered by the Intserv model is the interaction of a resource reservation protocol like RSVP with lower layer (i.e. link layer) resource reservation. For IntServ provision in a BSM network the concept of QID's (Queue Identifiers) at the SISAP is the concept used to provide this interaction with alternative link layers. QIDs represent abstract queues, each with a defined class of service, for transfer of IP packets to the SD layers. The satellite dependent lower layers are responsible for assigning satellite capacity and/or particular forwarding behaviour to these abstract queues according to defined properties.

Two main scenarios for the use of BSM resources in an IntServ network can be foreseen [17]:

1. **Static SD resources:** BSM SD resources for IntServ (i.e. high priority SD class) are provisioned and managed quasi-statically, and no interaction between RSVP and the SD resource control is available. A range of QIDs is however assumed to be available for specific use of IntServ and they may be of a range of data rates within the total SD resources.
2. **Dynamic SD resources:** BSM SD resources for IntServ are requested dynamically, and an interaction between RSVP and the SD resource control is available.

The functional architecture of the Ingress ST (either a remote ST or a Gateway ST, in the case of a star network) for dynamic SD resources is shown in Figure 8.

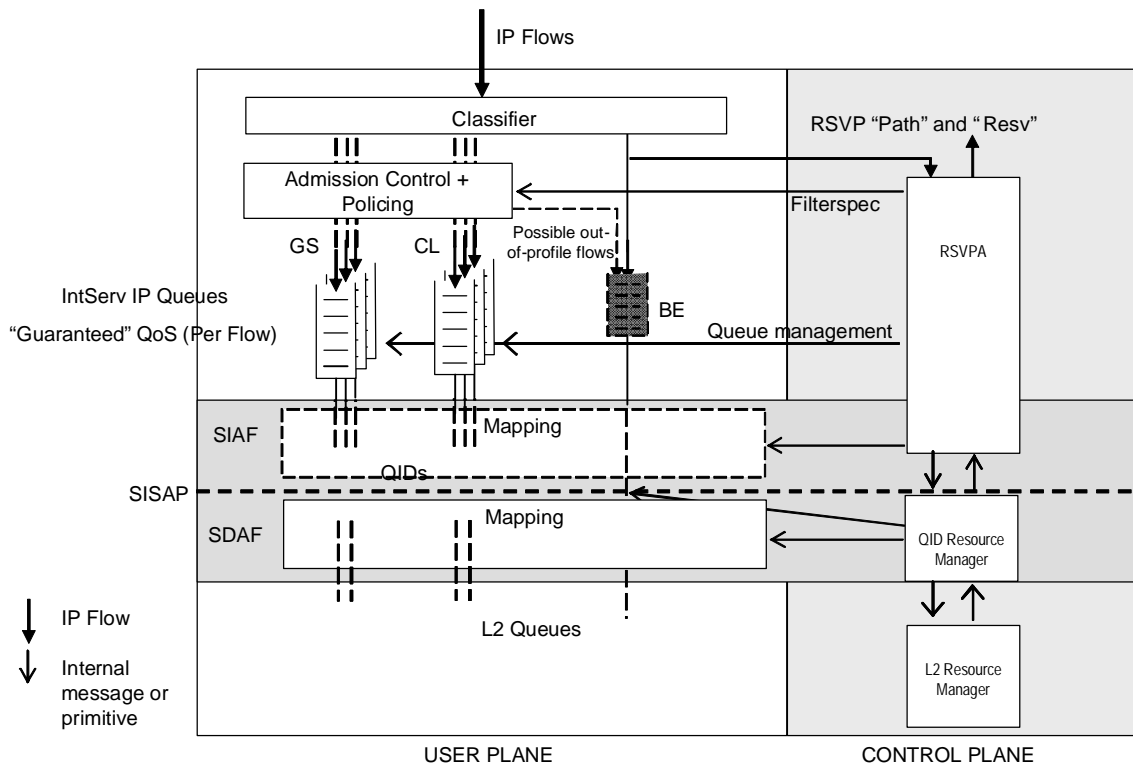


Figure 8: Ingress Architecture (Dynamic SD Resources)

### 5.1.7 Inter-working with DiffServ QoS

This subject aims at an open specification for enabling QoS for IP-based multimedia satellite systems, based on the DiffServ model. If IP packets entering the BSM network require a particular QoS treatment, they have to be mapped onto QIDs. The choice of the QID to be used inside the BSM network is thus particularly important. So the present document specifies the allocation of the QIDs and their mapping to IP QoS classes, when DiffServ is used to provide QoS at IP layer.

The technical standard document [18] describes in detail how QIDs are defined, how they are allocated and handled by the BSM network, and the requirements needed by sending and receiving Satellite Terminals (STs) in a BSM network to provide QID management functionalities. The document also defines the primitives that shall be used across the SI-SAP when allocating QIDs, when mapping DiffServ Code Points (DSCPs) and IP services to QIDs, when mapping QIDs to SD queues.

The functional architecture of the Ingress ST for DiffServ is shown in Figure 9.

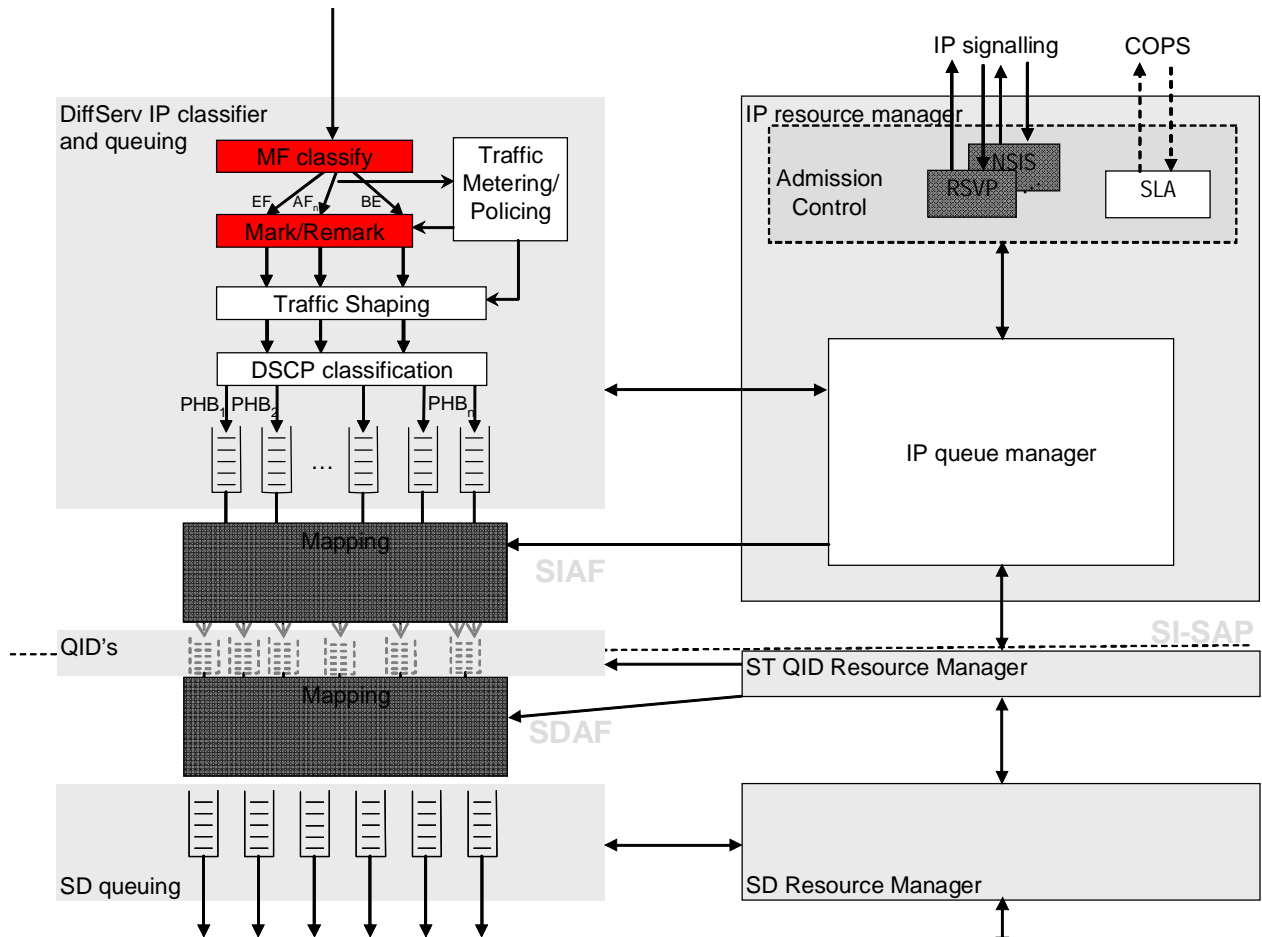


Figure 9: Detailed architecture of an ingress DiffServ-aware ST

### 5.1.8 General Security Architecture

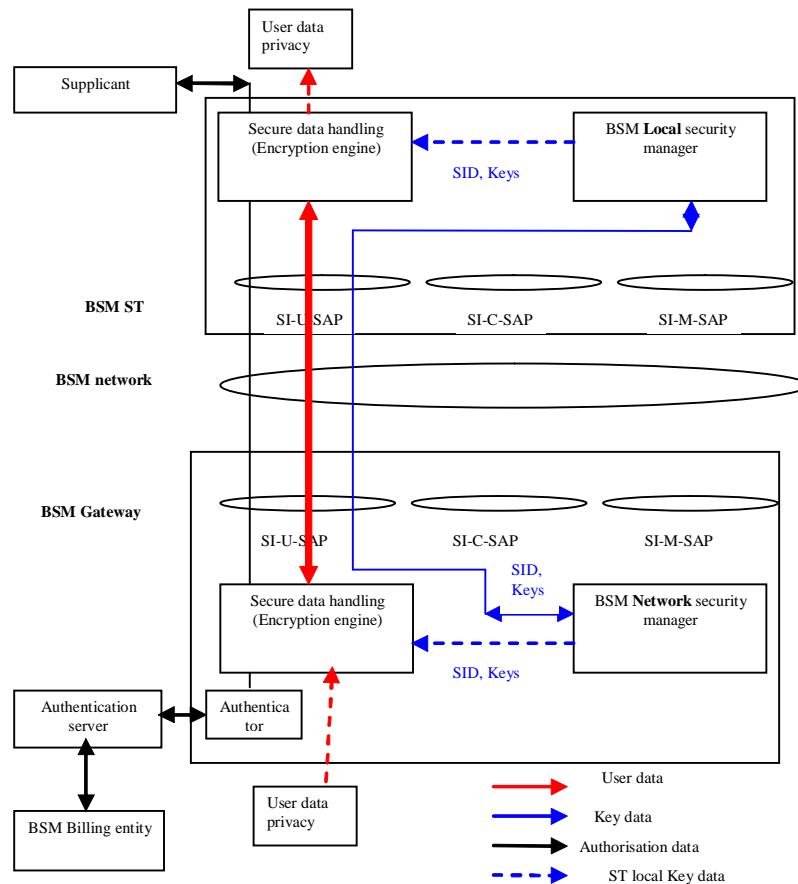
This section presents the detailed security system in various architectural cases [19]. These security cases are focused on the positioning of security functions above or below the SI-SAP. For example the security key management and data encryption entities can both be above or below the SI-SAP or one above and one below. In addition, the concept of BSM Security association Identity (SID) is presented. For example, if there is a secure connection between an ST and a Gateway, then SID is the reference number that is used to convey security information between **BSM Local and Network** security managers such as encryption keys, digital signature methods and security policy exchanges.

If there is only one single **BSM Network** security manager, then SID will be unique for the whole BSM network. If there are several **Network** security managers (for example one for each ISP), then SID must be used in conjunction with BSM-ID of the source and destination entities, in order to identify a security association between two BSM entities.

#### 5.1.8.1 BSM security architecture cases

The security cases presented here apply to both BSM star and mesh topologies. For a mesh topology with no On-Board Processor (OBP), STs communicate with each other through a BSM gateway (hub). For a mesh topology with OBP, STs communicate directly with each other without the need for the BSM Gateway (Hub). With respect to the security cases presented here, the star and mesh (no OBP) are the same, where the **BSM Network** security manager function is likely to be located at the BSM Gateway (Hub). However, for a mesh topology with OBP, the main difference is that **BSM Network** security manager function can be located at any BSM ST.

### 5.1.8.1.1 Case 1: IPsec and security entities in BSM



**Figure 10: Case 1 IPsec and BSM security entities**

As shown in Figure 10, this case illustrates the use of IPsec 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 BSM ST or Gateway). The security gateway consists of two functional entities:

1. Secure data handling entity (privacy/integrity engine): IPsec must operate in tunnel mode.
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.

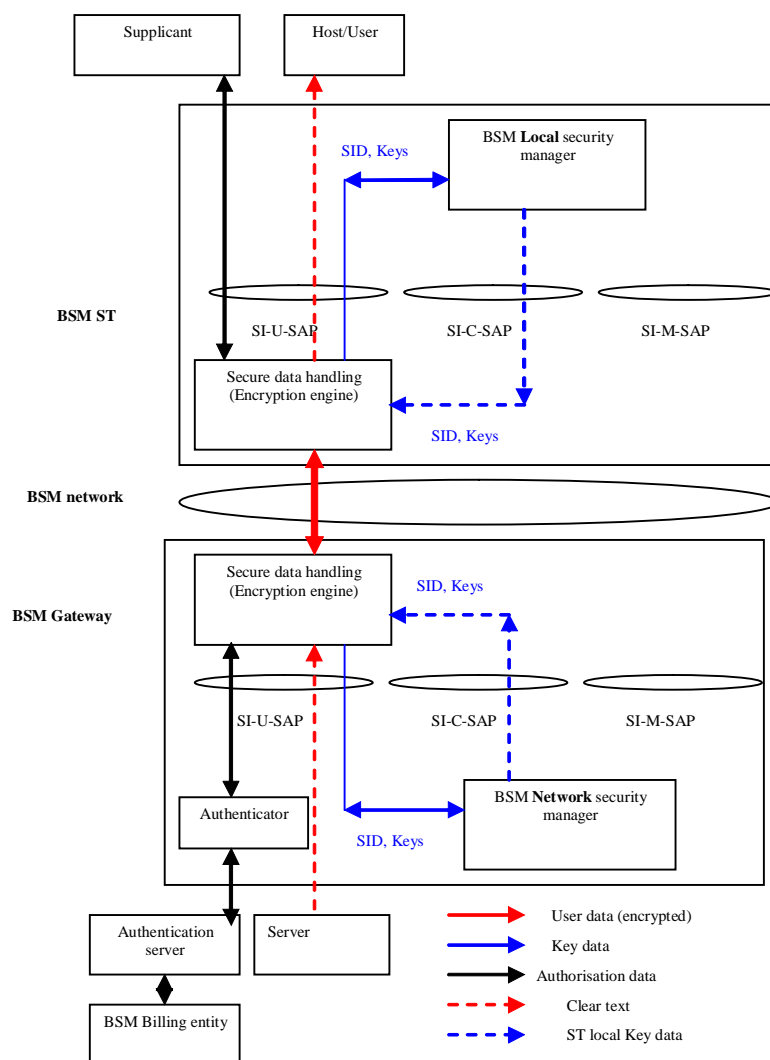
Figure 10 shows all security entities are above SI-SAP. The diagram also shows that the SI-U-SAP (the user interface) ONLY is used to communicate all secure information (user data and key management messages).

The client authentication process (supplicant, authenticator and Authentication server entities) is shown here as well, where IPsec is used to carry authentication information (such as user name and password) between Supplicant and authentication server.

Both the authentication server and the BSM network manager communicate with the BSM NCC regarding security and authorization. These interactions are not shown here in order to simplify the diagram. Registration and re-key security association must be established between the **BSM Network** security manager and **Local** security managers in each ST. In the case of IPsec, the IETF Internet Key Exchange (IKE) protocol (RFC 4109) must be used to establish all security associations. This will ensure the mutual authentication between all security entities, establishing the keys used subsequently to secure the user data. Using IKE will also ensure compatibility between BSM and the general Internet (terrestrial) security systems.

The Security association identity SID must be used in all security management message exchanges. However IPsec for multicast (star topology) is a challenge because IPsec tunnels must be set from the BSM gateways per ST. This is effectively a unicast configuration and the benefits of IP multicast are lost. Draft-ietf-msec-ipsec-extensions-02.txt is work in progress in defining the extra detail needed for IPsec to work efficiently with multicast. The Security Architecture for the Internet Protocol security architecture document (RFC 4301) 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-02.txt further defines the security services for manually and dynamically keyed IP multicast packets within that Security Architecture.

**5.1.8.1.2 Case 2: Mixed link layer security entities in BSM (security manager above SI-SAP and security engine below SI-SAP)**



**Figure 11: Case 2 Mixed link layer BSM security entities**

As shown in Figure 11, this case illustrates the use of link layer security (below SI-SAP) with the key management (security manager) as an application (above the SI-SAP in a star topology with a centralized security **Network** manager (can be co-located with the BSM gateway/hub). Typical

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

Like case 1, the security is provided between security gateways (can be co-located with BSM ST or Gateway). The security gateway consists of two functional entities:

1. Secure data handling entity (privacy/integrity engine): e.g. is DVB-RCS security which performs data encryption below SI-SAP
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 client authentication process (supplicant, authenticator and Authentication server entities) is shown here as well, where secure link layer is used to carry authentication information (such as user name and password) between supplicant and authentication server.

Figure 11 shows security entities above and below the SI-SAP. The diagram also shows that the SI-U-SAP (the user interface) is used to communicate secure user information, while the key management secure information is passed through the SI-C-SAP interface. The client authentication messages use the SI-U-SAP interface.

Both authentication server and the BSM **Network** manager communicate with the BSM NCC regarding security and authorization. These interactions are not shown here in order to simplify the diagram. Registration and re-key security association must be established between the **BSM Network** security manager and **Local** security manager in each ST. In the case of link layer security, the specific satellite systems security must be used. For example, for DVB-RCS satellite systems, the logon and key exchanges procedures of DVB-RCS recommendations [12] must be used to establish all security associations. For BSM systems operating with ULE, then the ULE specific key management procedures must be used (RFC 4326).

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 1).

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

#### **5.1.8.1.3 Case 3: End-to-end security**

This case is applicable to IPsec, TLS/SSL and application layer security (Figure 12). This is useful for end-to-end and remote access scenarios and is transparent to BSM network. If cases 1, 2 or 4 are used simultaneously with case 3, then a careful consideration must be paid to the BSM network performance degradation due to the dual security processing.

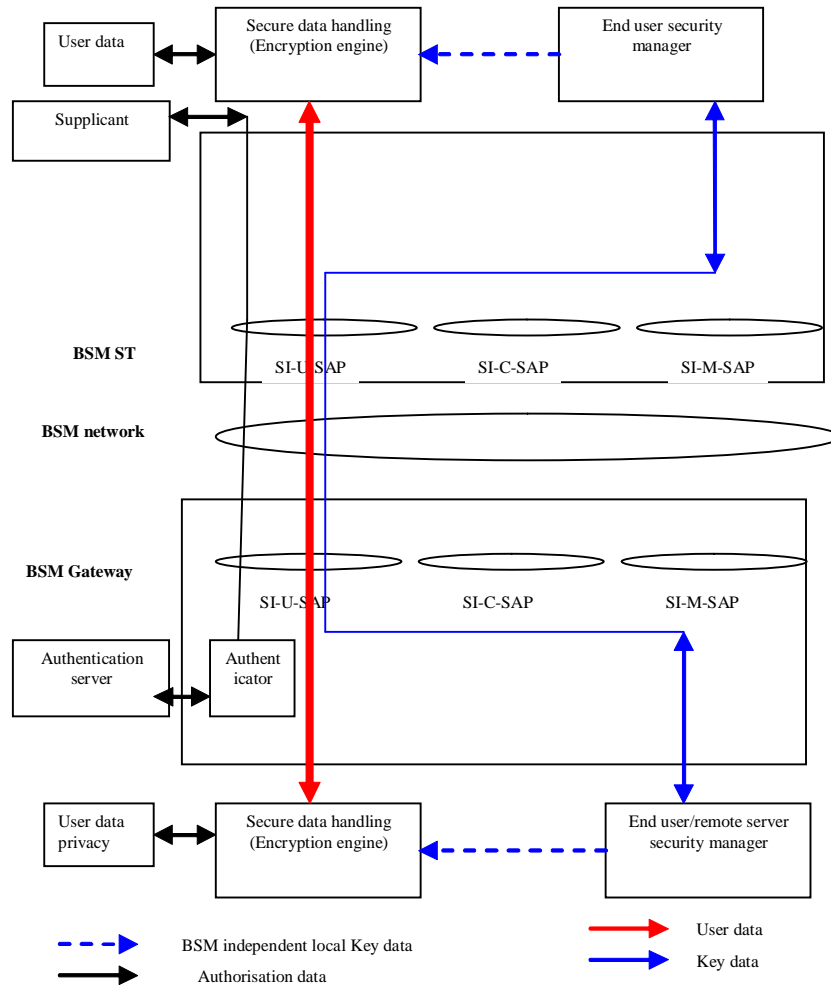


Figure 12: Case 3 End-to-end security, transparent to BSM

5.1.8.1.4 Case 4: Pure link layer security

This case(Figure 13) is applicable to ATM, DVB-RCS and ULE security systems that are implemented in the BSM network in the satellite link layer only. This case is transparent to BSM network. However, the BSM **Local** and **Network** security managers must be able to enforce the BSM security policy rules in this case such communication must use the SI-M-SAP interface. The Security association identity SID must be used in all security management message exchanges.

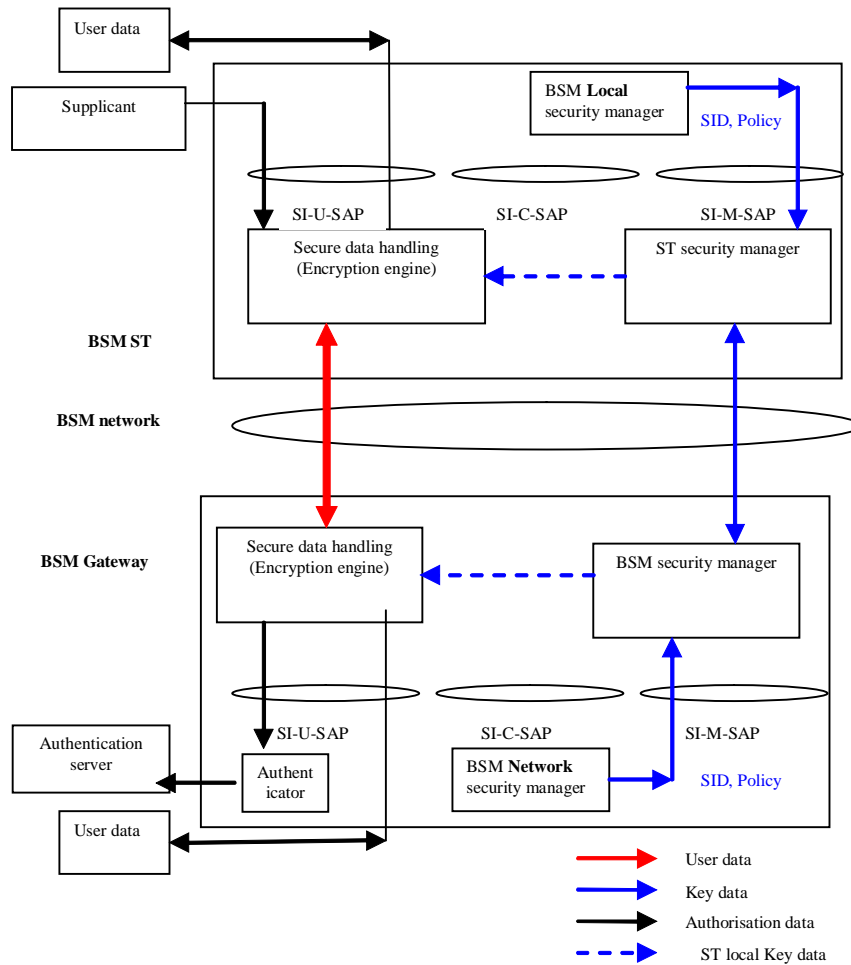
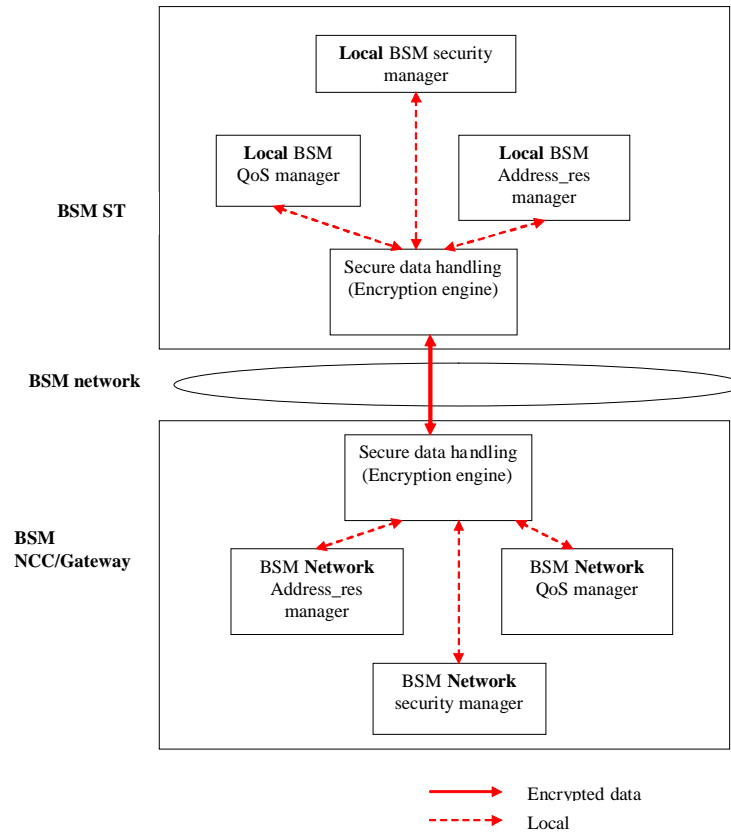


Figure 13: Case 4 link layer security, transparent to BSM

### 5.1.8.2 Generalized interactions between security and other BSM entities

This subsection addresses interaction and interworking with BSM QoS, address resolution management.

If QoS is used, then key management messages must use the high priority QoS classes to ensure fast and reliable key exchanges. This implies assigning QIDs with high class of service to security message exchanges. This applies to security cases 1, 2 and 3.



**Figure 14: Interaction between security, QoS and address resolution entities**

Figure 14 illustrates the use of BSM security to encrypt/authenticate QoS and Address resolution requests/responses between ST/Gateway and NCC. SI-SAP interfaces are not shown here because the focus of this diagram is securing message exchanges, over BSM network, between the **BSM Network** managers (QoS and address-resolution) and the **Local** manager in BSM ST/Gateway. The encryption engine can be below or above the SI-SAP.

Interactions between security and QoS entities

### 5.1.8.3 Security of QoS signalling in BSM network

The QoS functional architecture document (TS 102 462) presents QoS cases. In all these cases, it is assumed that the BSM system provides different levels of bearer QoS through a certain number of QIDs, which determine the nature of the QoS offered at the SI-SAP. It is the way in which the QIDs are accessed or modified by the IP layer and above that changes between cases. Security issues are the same in all these cases.

User and management planes are not addressed here. In the control plane, communications between the resource management in the ST/GW and the NCC must be secured. These QoS messages between the ST/GW and the NCC must be authenticated and optionally may be encrypted (this depends on the security policy for the BSM network).

In Figure 15 (copied from the QoS functional architecture document (TS 102 462); QoS case 3), if security is implemented below the SI-SAP, then link number 1 must be secured, using link layer such as DVB-RCS security procedures. If security is implemented above SI-SAP, then link number 2 must be secured, using IPsec or TLS security procedures. Either links 1 or 2 must be secured. However, it is possible to secure both links 1 and 2 at the same time, but the impact of security processing on BSM network performance must be assessed carefully in this situation.

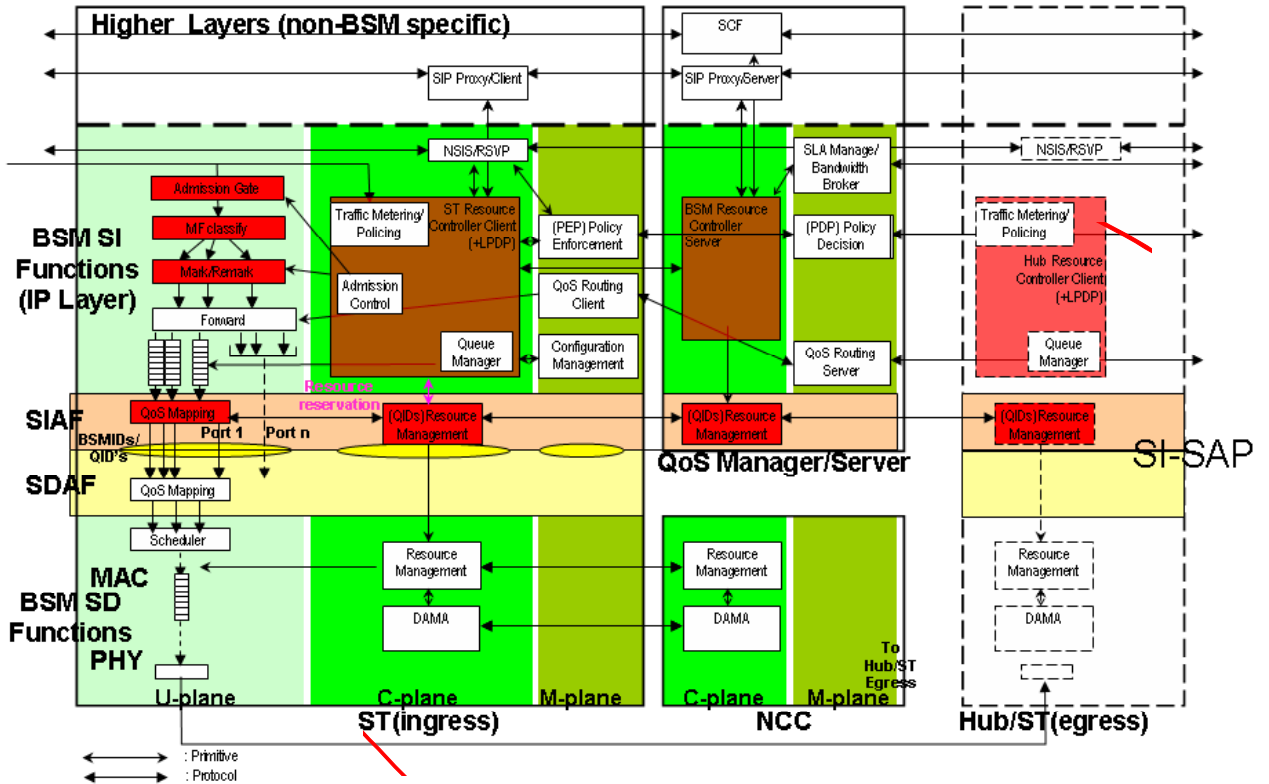


Figure 15: Securing Resource management messages between NCC and ST/GW

Also Figure 15 shows link number 3 between NSIS/SIP entities in the ST/GW and the NCC. The security issues for these entities are out of scope for BSM networks. However, if SIP or NSIS signalling is used in BSM, then the IETF security recommendations for both protocol must be observed (such as RFC 4081 for NSIS and RFC 3893 and RFC 3329 for SIP security).

#### 5.1.8.4 Using COPS protocol for security policy provisioning

In BSM networks, the Common Open Policy Service(COPS) protocol can be used to carry QoS or security information between BSM management entities and satellite terminals (gateways/ST) (RFC 2748). 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).

Figure 16 (from the QoS functional architecture document [16]; QoS case 3) shows the interaction between COPS entities to carry QoS and security related information. In the ST/Gateway, the Policy Enforcement Point (Policy-PEP) interacts with the **Local** security manager. In the NCC, the Policy Decision Point (Policy-PDP) will interact with BSM **Network** security manager. These interactions are not shown in the diagram for clarity.

The management plane is used to carry security policy related communications. Such communications do not need any special QoS treatment unless specified in the QoS or security policy rules.

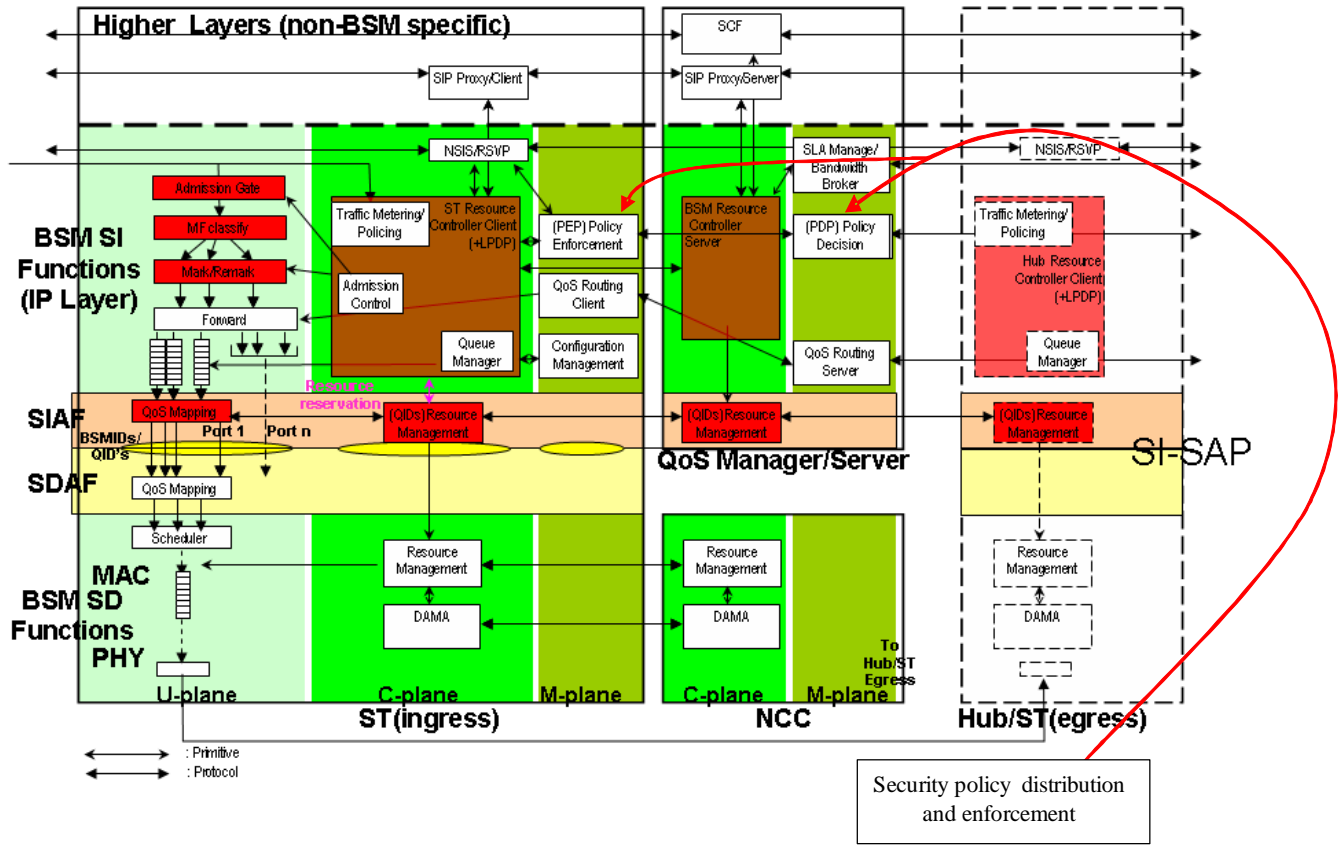


Figure 16: Securing policy distribution using COPS

**5.1.8.5 Using reliable transfer mechanisms (QoS) to transfer key management messages**

In security cases 1 and 3 the security management messages are transferred in the user plane through the SI-SAP interface. Therefore, the queues for security information are managed in the same way as any other user data. However, security management messages must be allocated a relatively high priority. Such allocation can be static and decided by the security policy of the BSM network or it can be dynamic depending on the nature of QoS offered at the SI-SAP.

Case 2 is similar to case 1 and 3, except that security key management messages are passed in the control plane through the SI-SAP interface. Therefore, a similar QoS management is needed in this plane for the security messages.

In case 4, all security management messages are below the SI-SAP. Therefore, there is no need for QoS management above the SI-SAP for these security messages.

**5.1.8.6 Interactions between security and address resolution entities**

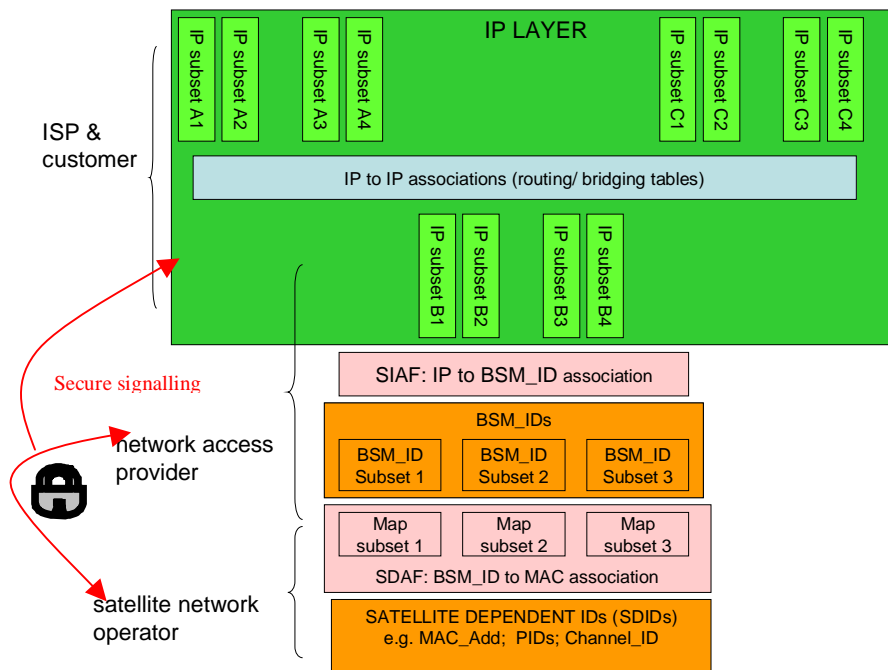
**5.1.8.6.1 Security of address resolution signalling in BSM network**

BSM address resolution is defined in the SI-SAP spec (TS 102 357) and the Address Management at the SI-SAP document (TS 102 460). The basic issues are how to map IP addresses to BSM-IDs and then to satellite specific MAC addresses.

A generalized model is shown in figure 20. Regarding security, any address resolution signalling across the SI-SAP interface within a single ST/Gateway or the NCC has no security implications.

However, communications between the address resolution entities (in ST/GW and the NCC) must be secured between ISPs, customers, network access providers and satellite network operators (as shown in Figure 17). These address resolution messages between the ST/GW and the NCC must be

authenticated and optionally may be encrypted (this depends on the security policy for the BSM network).



**Figure 17: Generalized Address management model in BSM network**

#### 5.1.8.6.1.1 Using RADIUS with DHCP servers

If DHCP is used in BSM, then the RADIUS Attributes sub-option enables a network element to pass identification and authorization attributes received during RADIUS authentication to a DHCP server (RFC 4014). When the DHCP server receives a message from a relay agent (Network Access Server, NAS) containing a RADIUS Attributes sub option, it extracts the contents of the sub option and uses that information in selecting configuration parameters for the client.

Transition to IPv6.

This Technical report studied the key issues for IPv6 introduction and produced recommendations for work on specific topics and standards in this area as follows:

- support for “native” IPv6 packets at the SI-SAP and in the Satellite dependent layers.
- use of dual-stack architecture above the SI-SAP.
- IPv6 Header Compression.
- IPv6 address mobility and any security implications arising.
- Management aspects and IPv6-aware Management Information Bases.
- IPv6 stateless auto-configuration (consequences of Unreachability Detection and Neighbour Discovery)
- revision of TS 102 460 (Address management at the SI-SAP) to take account of IPv6 issues.
- Multicast Source Management with a suitable IPv6-to-GID mapping scheme
- trade-offs for implementing and modifying the MLDvx protocols over BSM

## 5.2 IETF Working Group Documents

The IETF is responsible for network-layer and transport-layer protocols used in the general Internet. It also supports standardisation of link layer protocols required to support IP over specific technologies.

IETF specifications not only under-pin much of the work of the SATSIX project, but the project has actively participated in the standards process, ensuring that future Internet systems will interoperate with and over the link technologies developed in SATSIX./

### 5.2.1 Impact of SATSIX on IETF Standards

The IETF work has been actively supported by inputs from SATSIX partners. This standardisation is supported by active simulation and implementation work by the project – both essential components of the IETF standards process. This is due to the fact that SATSIX partners have acted, or are still acting, as co-authors, chairs and for several of the standards, namely:

<b>Standard</b>	<b>Author</b>
Address Resolution Mechanisms	<b>UoA</b>
Extension Formats for ULE and GSE	<b>UoA</b>
Security requirements for ULE	<b>UNIS</b>
Security Extension for ULE	<b>UNIS</b>
MIB for the UDP-Lite	<b>UoA</b>
The DCCP Service Code	<b>UoA</b>
Faster Restart for TFRC	<b>UoA</b>
Quick-Start for DCCP	<b>UoA</b>

### 5.2.2 Link-Layer Protocols

#### 5.2.2.1 Address Resolution Mechanisms for IP Datagrams over MPEG-2 Networks

This Informational RFC was published in 2007 as RFC 4947. G Fairhurst (University of Aberdeen) was a co-author. Mechanisms to perform address resolution for DVB are being studied in SATSIX, together with trials for the deployment of IPv6 over DVB networks.

This document describes the process of binding/associating IPv4/IPv6 addresses with MPEG-2 Transport Streams (TS). This procedure is known as Address Resolution (AR) or Neighbor Discovery (ND). Such address resolution complements the higher-layer resource discovery tools that are used to advertise IP sessions.

In MPEG-2 Networks, an IP address must be associated with a Packet ID (PID) value and a specific Transmission Multiplex. This document reviews current methods appropriate to a range of technologies (such as DVB (Digital Video Broadcasting), ATSC (Advanced Television Systems Committee), DOCSIS (Data-Over-Cable Service Interface Specifications), and variants). It also describes the interaction with well-known protocols for address management including DHCP, ARP, and the ND protocol.

#### 5.2.2.2 Extension Formats for Unidirectional Lightweight Encapsulation (ULE) and the Generic Stream Encapsulation (GSE)

This document describes a set of Extension Headers for the Unidirectional Lightweight Encapsulation (ULE), RFC4326. The Extension Header formats specified in this document define extensions appropriate to both ULE and the Generic Stream Encapsulation (GSE) defined to support the second generation framing structure defined by Digital Video Broadcasting (DVB) family of specifications.

The current document is intended for publication as a Proposed Standard RFC. One of the co-authors is with University of Aberdeen. Mechanisms to perform signalling at the link-layer for DVB-GSE are being defined and studied for future evolution of the DVB-RCS system in SATSIX. The document forms a part of the GSE specification being developed by DVB.

### **5.2.2.3 Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol**

The MPEG-2 standard defined by ISO 13818-1 supports a range of transmission methods for a range of services. This document provides a threat analysis and derives the security requirements when using the Transport Stream, TS, to support an Internet network-layer using Unidirectional Lightweight Encapsulation (ULE) defined in RFC4326. The document also provides the motivation for link-layer security for a ULE Stream. A ULE Stream may be used to send IPv4 packets, IPv6 packets, and other Protocol Data Units (PDUs) to an arbitrarily large number of Receivers supporting unicast and/or multicast transmission.

The current document draft-ietf-ipdvb-sec-req-04.txt is intended for publication as an Informational RFC. Two of the co-authors are with University of Surrey. This work directly supports work on security at the link-layer for DVB-RCS developed by SATSIX..

### **5.2.2.4 Security Extension for Unidirectional Lightweight Encapsulation Protocol**

This document describes a proposed the header extension for Unidirectional Encapsulation Protocol (ULE) that secures the IP traffic transported using ULE to provide security features like data confidentiality, data integrity, data origin authentication and mechanisms to prevent replay attacks. The format of the header extension and processing at the Receiver and Transmitter are described in detail.

The current document draft-cruikshank-ipdvb-sec-04.txt is intended for publication as a Proposed Standard RFC. Two of the co-authors are with University of Surrey. Mechanisms to perform security at the link-layer for DVB-RCS are being defined and implemented in the Platine testbed developed by SATSIX..

## **5.2.3 Transport Protocols**

### **5.2.3.1 MIB for the UDP-Lite protocol**

This document specifies a Management Information Base (MIB) module for the Lightweight User Datagram Protocol, RFC 3828. It defines a set of new MIB entities to characterise the behaviour and performance of transport layer endpoints deploying UDP-Lite. UDP-Lite resembles UDP, but differs from the semantics of UDP by the addition of a single option. This adds the capability for variable-length data checksum coverage, which can benefit a class of applications that prefer delivery of (partially) corrupted datagram payload data in preference to discarding the datagram.

The document is intended for publication as a Proposed Standard RFC. Both authors are with University of Aberdeen. It describes a new MIB for multimedia transport over the Internet. This publication resulted from earlier implementation work in SATSIX.

### **5.2.3.2 The DCCP Service Code**

This document describes the usage of Service Codes by the Datagram Congestion Control Protocol, RFC 4340. This document motivates the setting of Service Codes by applications. Service Codes

provide a method to identify the intended service/application to process a DCCP connection request. This provides improved flexibility in the use and assignment of port numbers for connection multiplexing. The use of a DCCP Service Code can also enable more explicit coordination of services with middleboxes (e.g. network address translators and firewalls). It updates the description provided in RFC 4340.

The document is intended for publication as a Proposed Standard RFC. The author is with University of Aberdeen. It describes new protocol mechanisms for multimedia over the Internet that resulted from implementation of open-source DCCP support in Linux. This implementation was developed in SATSIX, and will be used to evaluate the emulation platform.

### **5.2.3.3 Faster Restart for TCP Friendly Rate Control (TFRC)**

TCP-Friendly Rate Control (TFRC) is a congestion control mechanism for unicast flows operating in a best-effort Internet environment. This document introduces Faster Restart, an optional mechanism for safely improving the behavior of interactive flows that use TFRC. Faster Restart is proposed for use with TFRC and with TFRC-SP, the Small Packet variant of TFRC. We present Faster Restart in general terms as a congestion control mechanism, and further describe how to implement Faster Restart in Datagram Congestion Control Protocol (DCCP) Congestion Control IDs 3 and 4.

The current document is intended for publication as an Experimental RFC. One of the co-authors is with University of Aberdeen. Mechanisms to enhance multimedia performance over links with appreciable delay are being defined and simulated in WP2500 in SATSIX.

### **5.2.3.4 Quick-Start for DCCP**

The Datagram Congestion Control Protocol (DCCP) is a transport protocol that allows the transmission of congestion-controlled, unreliable datagrams. It is intended for applications such as streaming media, Internet telephony, and on-line games. In DCCP, an application has a choice of congestion control mechanisms, each specified by a Congestion Control Identifier (CCID). This document specifies a framework for the use of the Experimental Quick-Start mechanism by DCCP, and specific procedures for the use of Quick-Start with DCCP CCID-2 and CCID-3.

The current document is intended for publication as an Experimental RFC. The two co-authors are with University of Aberdeen. Mechanisms to perform QoS and cross-layer methods to support the link-layer for DVB-RCS are being defined and simulated in WP2500 in SATSIX.

## **5.3 DVB-RCS Technical Module Working Group**

DVB-RCS standardization group was re-opened early this year to accomplish DVB-RCS mobile. Finally, a new version of the standard EN 301 790 v1.5.1 will be issued in January 2008, including DVB-RCS mobile LOS (Line Of Sight) and nLOS (non Line Of Sight) specifications, small clarifications and the impact of C2P, Connection Control Protocol, for DVB-RCS mesh networking.

The interest of SatSix project in the follow up of TM-RCS activities has been mainly due to C2P and mesh networking, but also the different handover mechanism and future NCC handover mechanisms to be synchronized with the studies done in satellite network mobility.

## CONCLUSIONS

This document presents the standardisation activities performed during the **SATSIX** Project. **SATSIX** has helped to establish a range of ETSI technical standards covering a range of issues focussed on IP services provision over networks with integrated satellite sub-networks. These generic standards have been further employed in **SATSIX** as a basis for its own specific solutions to network implementation.

## 6 REFERENCES

- [1] Security requirements for the Unidirectional Lightweight Encapsulation (ULE) protocol in the ipdvb working group: draft-ietf-ipdvb-sec-req-03.txt. Latest version submitted in June 2007.
- [2] Maravedis, "Wi-Max and broadband wireless (sub 11 Ghz) Worldwide market analysis and trend 2005-2010"
- [3] ETSI TR 101 329-7: "Telecommunications and Internet Protocol Harmonisation over Networks (TIPHON); End to End Quality of Service in TIPHON system; Design Guide for Elements of a TIPHON connection from an end-to-end speech transmission performance point view".
- [4] SATIP6, "Satellite/IPv6 Network System Scenarios", 2001.
- [5] WiMAX Forum.; "WiMAX End-to-End Network System Architecture, Stage 3: Detailed Protocols and Procedures", progress draft Aug 2006.
- [6] IEEE STD 802.16-2004: "Air Interface for fixed Broadband Wireless Access Systems", Oct 2004.
- [7] IEEE P802.16e/D12: "Air Interface for Fixed and Mobile Broadband Wireless Access Systems", Feb 2005.
- [8] WiMax Forum: "Mobile WiMAX- Part: A Technical Overview and Performance Evaluation", Feb 2006.
- [9] IETF Draft: "Transmission of IP Packets over Ethernet over IEEE802.16", draft-riegel-16ng-ip-over-eth-over-80216-00.txt, Jun 2006.
- [10] IETF Draft: "Transmission of IPv6 over 802.16's IPv6 Convergence Sublayer", draft-madanapalli-ipv6-over-802.16-ipv6cs-00.txt, Jun 2006.
- [11] ECMA: "Corporate Telecommunication Networks – Mobility for Enterprise Communications" Technical Report ECMA TR/92, Dec 2005.
- [12] ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".
- [13] ETSI TS 102 357 "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Common air interface specification: Satellite Independent Service Access Point (SI-SAP)"
- [14] TS 102 460: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; Address Management at the SI-SAP".
- [15] TS 102 461: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; Multicast Source Management".
- [16] TS 102 462: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; QoS Functional Architecture".
- [17] TS 102 463: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; Interworking with IntServ QoS".
- [18] TS 102 464: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; Interworking with DiffServ QoS".
- [19] TS 102 465: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; General Security Architecture".
- [20] TS 102 466: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; Multicast Security Architecture".
- [21] TR 102 467: "Satellite Earth Station and systems (SES); Broadband Satellite Multimedia; IPv6 Transition"
- [22] ETSI TS 185 001 "NGN; QoS Framework and Requirements"
- [23] ETSI home page: [http://portal.etsi.org/Portal\\_Common/home.asp](http://portal.etsi.org/Portal_Common/home.asp)
- [24] Multicast IP Security Composite Cryptographic Groups in the msec working group: draft-ietf-msec-ipsec-composite-group-01. Latest version submitted in June 2007.