



***Society of Cable  
Telecommunications  
Engineers***

---

**ENGINEERING COMMITTEE  
Data Standards Subcommittee**

---

**AMERICAN NATIONAL STANDARD**

**ANSI/SCTE 169-2 2010**

**IPCablecom SMA Part 2: Security, Monitoring, and  
Automation Specification**

---

## NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members, whether used domestically or internationally.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the Standards. Such adopting party assumes all risks associated with adoption of these Standards, and accepts full responsibility for any damage and/or claims arising from the adoption of such Standards.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this standard have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2010  
140 Philips Road  
Exton, PA 19341

---

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

---

# Contents

|                |                                                             |           |
|----------------|-------------------------------------------------------------|-----------|
| <b>1</b>       | <b>SCOPE.....</b>                                           | <b>1</b>  |
| 1.1            | Introduction and Purpose.....                               | 1         |
| 1.2            | Requirements .....                                          | 1         |
| <b>2</b>       | <b>REFERENCES .....</b>                                     | <b>2</b>  |
| 2.1            | Normative References .....                                  | 2         |
| 2.2            | Informative References.....                                 | 3         |
| 2.3            | Reference Acquisition .....                                 | 3         |
| <b>3</b>       | <b>TERMS AND DEFINITIONS .....</b>                          | <b>4</b>  |
| <b>4</b>       | <b>ABBREVIATIONS AND ACRONYMS.....</b>                      | <b>5</b>  |
| <b>5</b>       | <b>OVERVIEW .....</b>                                       | <b>6</b>  |
| 5.1            | IPCablecom SMA .....                                        | 6         |
| 5.2            | SMA Functional Entities .....                               | 7         |
| 5.3            | SMA Functional Areas .....                                  | 8         |
| 5.3.1          | Signaling.....                                              | 8         |
| 5.3.2          | Media Session Establishment .....                           | 8         |
| 5.3.3          | QoS .....                                                   | 9         |
| 5.3.4          | Security .....                                              | 9         |
| <b>6</b>       | <b>IPCABLECOM SMA SIGNALING INTERFACE REQUIREMENTS.....</b> | <b>10</b> |
| 6.1            | SMA Signaling .....                                         | 11        |
| 6.1.1          | HTTP Protocol Usage and URI Formation.....                  | 11        |
| 6.1.2          | SMA Messages .....                                          | 12        |
| 6.1.3          | Registration and Deregistration.....                        | 15        |
| 6.1.4          | Heartbeat .....                                             | 16        |
| 6.1.5          | Error Handling.....                                         | 17        |
| 6.1.6          | Backoff and Retry Procedures .....                          | 18        |
| 6.1.7          | SMA Logic .....                                             | 19        |
| 6.2            | Media .....                                                 | 19        |
| 6.2.1          | HTTP URI usage .....                                        | 21        |
| 6.2.2          | Transport .....                                             | 21        |
| 6.2.3          | Codecs .....                                                | 21        |
| 6.2.4          | NAT and Firewall traversal.....                             | 21        |
| 6.3            | Quality of Service .....                                    | 22        |
| 6.3.1          | QoS Usage .....                                             | 23        |
| 6.3.2          | Procedures.....                                             | 23        |
| 6.4            | Security .....                                              | 24        |
| 6.4.1          | Authentication.....                                         | 24        |
| 6.4.2          | Message Integrity and Protection.....                       | 25        |
| 6.4.3          | TLS Profile.....                                            | 25        |
| 6.4.4          | TLS Certificate Profile and Validation.....                 | 25        |
| <b>ANNEX A</b> | <b>SMA DATA MODELS (NORMATIVE).....</b>                     | <b>27</b> |
| A.1            | Instruction.....                                            | 27        |
| A.2            | Event.....                                                  | 27        |
| A.3            | Registration.....                                           | 28        |
| A.4            | Deregistration .....                                        | 28        |
| A.5            | Response.....                                               | 29        |

---

|                     |                                                                                |           |
|---------------------|--------------------------------------------------------------------------------|-----------|
| A.6                 | Device List.....                                                               | 29        |
| A.7                 | Heartbeat.....                                                                 | 30        |
| A.8                 | Logic.....                                                                     | 30        |
| A.9                 | Device Profile.....                                                            | 34        |
| <b>ANNEX B</b>      | <b>SMA LOGIC (NORMATIVE) .....</b>                                             | <b>45</b> |
| B.1                 | Macros and Statements .....                                                    | 45        |
| B.2                 | Assignments.....                                                               | 45        |
| B.3                 | Method/Macro Invocation .....                                                  | 46        |
| B.4                 | Wait Statement .....                                                           | 46        |
| B.5                 | Local Variable Usage .....                                                     | 46        |
| B.6                 | Expressions.....                                                               | 46        |
| B.7                 | Conditionals.....                                                              | 47        |
| B.8                 | If-Else .....                                                                  | 47        |
| B.9                 | While .....                                                                    | 48        |
| B.10                | Until .....                                                                    | 48        |
| B.11                | Switch .....                                                                   | 48        |
| B.12                | Temporal Expressions .....                                                     | 48        |
| B.13                | Return Values From a Macro .....                                               | 49        |
| B.14                | Triggers.....                                                                  | 50        |
| B.15                | Schedules .....                                                                | 50        |
| <b>APPENDIX I</b>   | <b>SMA SIGNALING EXAMPLES .....</b>                                            | <b>51</b> |
| I.1                 | Retrieve a specific property of an SMA device .....                            | 51        |
| I.2                 | To retrieve all properties specific to an SMA device .....                     | 52        |
| I.3                 | Retrieving a specific set of properties for an SMA device .....                | 52        |
| I.4                 | To retrieve all properties of all SMA devices connected to an SMA gateway..... | 53        |
| I.5                 | Retrieve an SMA gateway's devices, capabilities and macros.....                | 54        |
| I.6                 | Updating a Property.....                                                       | 55        |
| <b>APPENDIX II</b>  | <b>SMA LOGIC EXAMPLES .....</b>                                                | <b>56</b> |
| II.1                | Example 1 .....                                                                | 56        |
| II.1.1              | Example 1a .....                                                               | 56        |
| II.1.2              | Example 1b .....                                                               | 56        |
| II.2                | Example 2 .....                                                                | 56        |
| II.3                | Example 3 .....                                                                | 56        |
| II.4                | Example 4 .....                                                                | 57        |
| II.5                | Example 5 .....                                                                | 57        |
| <b>APPENDIX III</b> | <b>SMA DEVICE PROFILE USAGE .....</b>                                          | <b>59</b> |
| III.1               | Example Light Switch XML Schema.....                                           | 59        |
| III.2               | Example Device Listing .....                                                   | 60        |

---

# Figures

Figure 1 - SMA Reference Architecture.....6

Figure 2 - SMA Entities and Interactions.....7

Figure 3 - SMA Interfaces .....10

Figure 4 - SMA Signaling Interface .....11

Figure 5 - SMA Media Session Establishment.....20

Figure 6 - Interfaces to support media in the presence of NATs.....22

Figure 7 - SMA QoS Interfaces.....22

# Tables

Table 1 - Event Server behavior upon receiving HTTP responses from the SMA gateway .....17

Table 2 - SMA gateway behavior upon receiving HTTP responses from the Event Server .....17

Table 3 - QoS Interface Descriptions .....23

Table 4 - TLS Certificate Profile .....25

---

This page is left blank intentionally.



---

# 1 SCOPE

## 1.1 Introduction and Purpose

IPCablecom SMA is designed to address the following areas.

- **Security** - The ability to protect lives and property through professional monitoring, notifying first responders (e.g., fire, police, and medical) and providing emergency alerts to authorized individuals like home occupants. For example, fire and smoke sensors alert monitoring agencies who can notify and provide critical information to local emergency personnel.
- **Monitoring** - The ability to self-monitor the status and activity in the home so that a user can be made aware of any desired state changes. For example, when motion is detected by a motion sensor, real-time alerts such as video or photo clips are transmitted to the desired recipients.
- **Automation** - The ability to automate and remotely control lifestyle conveniences such as lighting, heating, cooling and appliances. For example, a user can remotely use a web portal to verify and control conditions such as lighting or temperature in the home.

This document specifies the Signaling, Media, Quality of Service (QoS), and Security requirements to support the PacketCable SMA Architecture. For the SMA gateway device architecture, provisioning and management requirements please refer to [SMA-PROV].

## 1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

|              |                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "MUST"       | This word means that the item is an absolute requirement of this specification.                                                                                                                                                                                                   |
| "MUST NOT"   | This phrase means that the item is an absolute prohibition of this specification.                                                                                                                                                                                                 |
| "SHOULD"     | This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.                                                             |
| "SHOULD NOT" | This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. |
| "MAY"        | This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.                                                  |

---

## 2 REFERENCES

The following documents contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

### 2.1 Normative References

- |                   |                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ID ICE]          | IETF Internet-Draft, draft-ietf-mmusic-ice-19, Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, October 29, 2007, work in progress. |
| [ID TURN]         | IETF Internet-Draft, draft-ietf-behave-turn-11, Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), October 29, 2008, work in progress.                             |
| [PKT-CODEC-MEDIA] | PacketCable 2.0 Codec and Media Specification, PKT-SP-CODEC-MEDIA-I05-080710, July 10, 2008, Cable Television Laboratories, Inc.                                                                                          |
| [MM]              | ANSI/SCTE 159-1 2010, Multimedia Application and Service Part 1: IP Cablecom Multimedia.                                                                                                                                  |
| [MM-WS]           | ANSI/SCTE 159-2 2010, IP Cablecom Multimedia Part 2: Multimedia Web Service Interface                                                                                                                                     |
| [SEC1.5]          | ANSI/SCTE 165-10 2009, IP Cablecom 1.5 Part 10: Security Specification                                                                                                                                                    |
| [SMA-PROV]        | ANSI/SCTE 169-3 2010, IP Cablecom SMA Part 3: Security, Monitoring, and Automation Provisioning Specification.                                                                                                            |
| [RFC 2616]        | IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, June 1999.                                                                                                                                                        |
| [RFC 2617]        | IETF RFC 2617, HTTP Authentication: Basic and Digest Access Authentication, June 1999.                                                                                                                                    |
| [RFC 2818]        | IETF RFC 2818, HTTP over TLS, May 2000.                                                                                                                                                                                   |
| [RFC 3264]        | IETF RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP), June 2002.                                                                                                                              |
| [RFC 3268]        | IETF RFC 3268, Advanced Encryption Standard (AES) cipher suites for Transport Layer Security (TLS), June 2002.                                                                                                            |
| [RFC 4346]        | IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, April 2006.                                                                                                                                       |
| [RFC 4566]        | IETF RFC 4566, SDP: Session Description Protocol, July 2006.                                                                                                                                                              |
| [RFC 5280]        | IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.                                                                                              |
| [RFC 5389]        | IETF RFC 5389, Session Traversal Utilities for NAT (STUN), October 2008.                                                                                                                                                  |
| [W3 XML1.0]       | Extensible Markup Language (XML) 1.0 (Fourth Edition), W3C Recommendation, August 2006.                                                                                                                                   |
| [W3 XSD1.0]       | XML Schema Part 1: Structures Second Edition, W3C Recommendation 28, October 2004.                                                                                                                                        |

---

## 2.2 Informative References

This specification uses the following informative references.

- |                 |                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ID-ICE-NONSIP] | IETF Internet-Draft, draft-rosenberg-mmusic-ice-nonsip-01, "Guidelines for Usage of Interactive Connectivity Establishment (ICE) by non Session Initiation Protocol (SIP) Protocols", July 14, 2008, work in progress. |
| [TR-MM-ARCH]    | PacketCable Multimedia Architecture Framework Technical Report, PKT-TR-MM-ARCH-V02-051221, December 21, 2005, Cable Television Laboratories, Inc.                                                                      |
| [TR-PKT-NFT]    | PacketCable NAT and Firewall Traversal Technical Report, PKT-TR-NFT-V05-080425, April 25, 2008, Cable Television Laboratories, Inc.                                                                                    |
| [TR-SMA]        | SCTE 169-1 2010, SMA Part 1: Architecture Framework Technical Report                                                                                                                                                   |

## 2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; <http://www.cablelabs.com>
- Internet Engineering Task Force (IETF), Internet: <http://www.ietf.org/>  
Note: Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time.  
The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.  
Internet-Drafts may also be accessed at <http://tools.ietf.org/html/>
- World Wide Web Consortium, [www.w3c.org](http://www.w3c.org), c/o MIT, 32 Vassar Street, Room 32-G515, Cambridge, MA 0213.

---

### 3 TERMS AND DEFINITIONS

This specification uses the following terms:

|                              |                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Conditional</b>           | An XML element that provides for conditional execution of statements                                                                                                                                                            |
| <b>DSx Signaling</b>         | DSA, DSC, and DSD – the full range of Dynamic Service messaging                                                                                                                                                                 |
| <b>Event</b>                 | A change in a defined condition                                                                                                                                                                                                 |
| <b>Expression</b>            | An XML element that resolves to a value                                                                                                                                                                                         |
| <b>Macro</b>                 | A series of steps and logic that can be run                                                                                                                                                                                     |
| <b>NAT, NAPT</b>             | NATs perform IP address translation, typically interconnecting private and public address domains. NAPT devices also translate ports in order to save IP addresses. In this document, the term NAT also refers to NAPT devices. |
| <b>IPCablecom Multimedia</b> | An application agnostic QoS architecture for services delivered over DOCSIS networks                                                                                                                                            |
| <b>RESTful web services</b>  | Use of REST design principles via HTTP as the protocol                                                                                                                                                                          |
| <b>Schedule</b>              | A time-based event generator                                                                                                                                                                                                    |
| <b>Statement</b>             | A single step in a macro                                                                                                                                                                                                        |
| <b>Trigger</b>               | Something that responds to an event by running a program                                                                                                                                                                        |

---

## 4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

|                |                                                  |
|----------------|--------------------------------------------------|
| <b>AS</b>      | Application Server                               |
| <b>AM</b>      | Application Manager                              |
| <b>CM</b>      | Cable Modem                                      |
| <b>CMTS</b>    | Cable Modem Termination System                   |
| <b>DOCSIS®</b> | Data-Over-Cable Service Interface Specifications |
| <b>HTTP</b>    | Hyper Text Transport Protocol                    |
| <b>ICE</b>     | Interactive Connectivity Establishment           |
| <b>IP</b>      | Internet Protocol                                |
| <b>MPEG</b>    | Moving Picture Experts Group                     |
| <b>NAT</b>     | Network Address Translation                      |
| <b>PCMM</b>    | PacketCable Multimedia                           |
| <b>PS</b>      | Policy Server                                    |
| <b>QoS</b>     | Quality of Service                               |
| <b>REST</b>    | REpresentational State Transfer                  |
| <b>SMA</b>     | Security, Monitoring and Automation              |
| <b>SMS</b>     | Short Message Service                            |
| <b>STUN</b>    | Simple Traversal of UDP Through NAT              |
| <b>TLS</b>     | Transport Layer Security                         |
| <b>TURN</b>    | Traversal Using Relay NAT                        |
| <b>XML</b>     | eXtensible Markup Language                       |

## 5 OVERVIEW

The PacketCable Security, Monitoring and Automation (SMA) architecture describes a set of functional groups and logical entities, as well as a set of interfaces that support the information flows exchanged between the entities.

This section provides:

- An overview of IPCablecom SMA.
- An overview of the functional entities and areas addressed by this specification.

The remainder of this section provides an brief overview of IPCablecom SMA, the functional area and entities. Please refer to [TR-SMA] for a detailed overview of IPCablecom SMA.

### 5.1 IPCablecom SMA

IPCablecom SMA, as specified in this document identifies a set of functional groups and logical entities as illustrated in Figure 1.

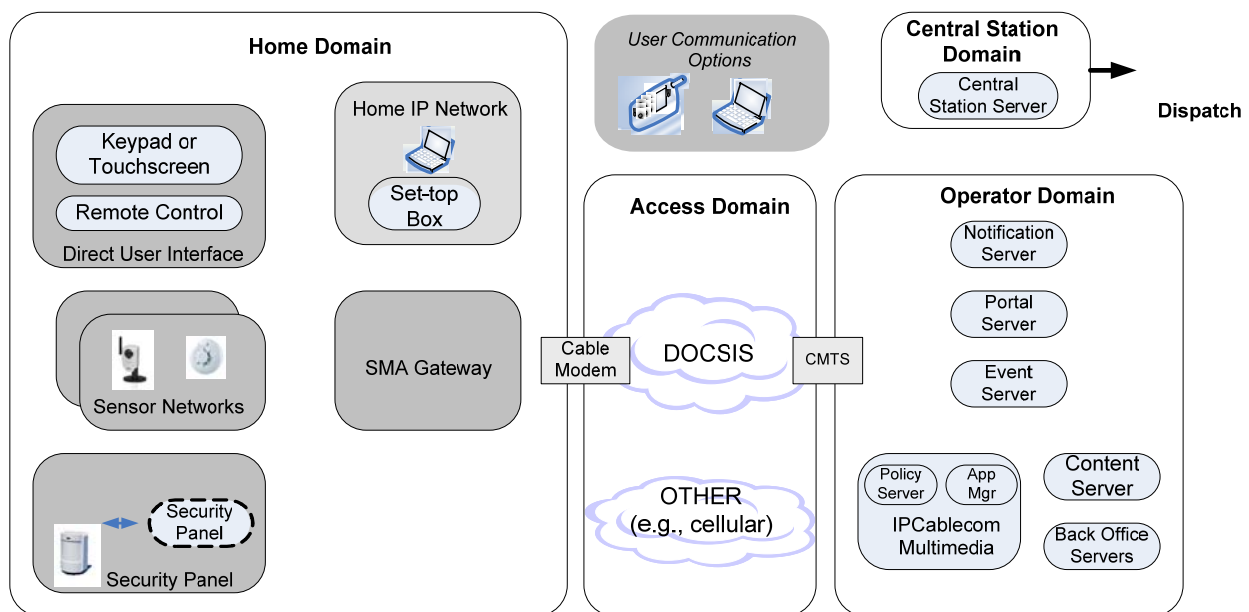


**Figure 1 - SMA Reference Architecture**

There are four domains that are identified, as described below:

- **Home Domain:** The Home Domain consists of the SMA gateway which communicates with servers in the Operator Domain as well as entities in the home such as legacy security panels, sensors and controller networks, home Internet protocol (IP) networks, and user interfaces (keypads, remote controls, Set-top Box OCAP application, etc.).
- **Access Domain:** The Access Domain provides the communications path and QOS resources required to facilitate communications between the SMA gateway and the Operator Domain. The Access Domain includes the Cable Modem, and optional router, in the home as well as the Cable Modem Termination System in the network.

- **Operator Domain:** The Operator Domain contains an Event Server which communicates with the SMA gateway. It also contains a Portal Server which allows the end user to check status, arm/disarm, and manage the system through various interfaces such as web user interface. Other elements in the Operator Domain include Operational Support Systems to facilitate billing, provisioning, customer care, and network management.
- **Central Station Domain:** The Central Station Domain contains hardware, software and communications facilities required to receive critical alarms from the Event Server.

## 5.2 SMA Functional Entities

Figure 2 depicts typical SMA entities and their relationships, as relevant to the IPCablecom SMA efforts. For simplicity, the diagram indicates two domains, Operator and Home. Each domain contains a set of logical or physical components.

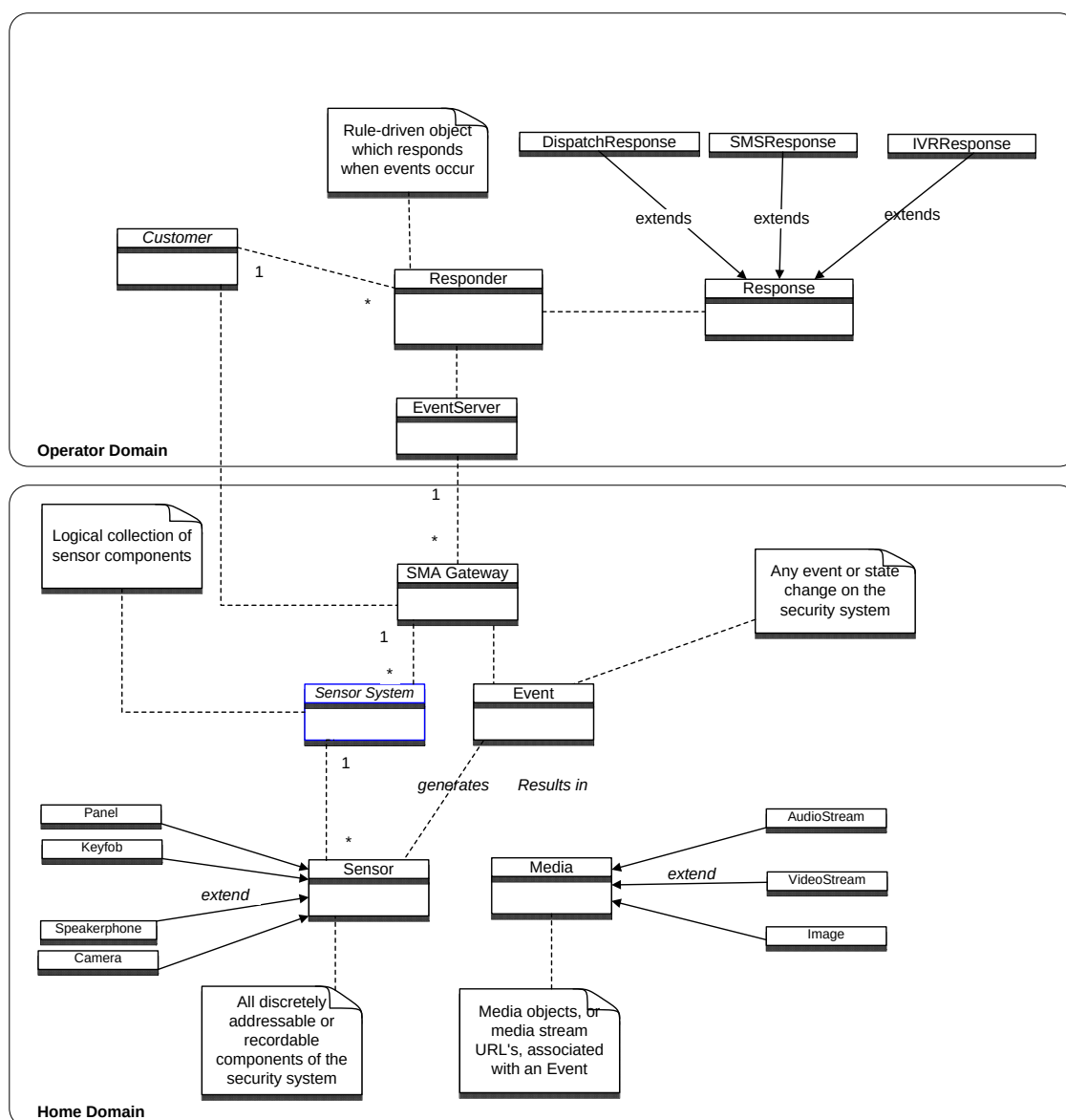


Figure 2 - SMA Entities and Interactions

---

IPCablecom SMA specified in this document focuses on the interface between two primary entities: the SMA gateway and the Event Server. The SMA gateway resides in the customer premises, and acts as the conduit to signaling interactions between the Operator and the SMA devices in the home. Communication from the Operator domain is accomplished using the Event Server, the SMA gateway's counterpart in the MSO domain.

In the customer premise, the SMA gateway is responsible for communications with one or more security systems ("System"). Each System is a logical collection of one or more Components in the security system. Each Component, in turn, represents Controls, Sensors, or both. Examples of Sensors include magnets (for doors and windows), motion sensors, speakerphones (for listening in), and video cameras. These sensors are primarily unidirectional, reporting state or other sensory information to the Gateway, but not accepting state changes.

Controls are similar to Sensors in that they represent devices deployed throughout the home. Controls are also controllable, accepting requests for state changes from the SMA gateway. Examples of Controls include Lighting controls, and the security Panel itself (arming and disarming it).

When a Security System detects a state change (e.g., in a sensor), it reports a security Event, a data object which identifies the sensor and the state change. Each Event may be associated with one or more media data objects, to include rich media information which is contextual to the event. Media types can be audio streams, video streams, or still images.

The Event Server receives all events from the SMA gateway. When an Event is received, the Event Server will iterate through one or more processing rules, termed Responders, which are rule-driven objects that listen for Events of certain kinds, and respond appropriately. For example, one Responder might watch for Burglary events, and respond with "dispatch the Police". Another Responder might watch for Arming or Disarming events, and respond with "send an SMS message to the customer". Each of these types of responses (dispatch, SMS, etc.) are represented by Response objects, for which three specific sample types are shown: Dispatch Response, SMS Response, and IVR Response (IVR stands for "Interactive Voice Response", also known as "automated outbound phone call").

## 5.3 SMA Functional Areas

IPCablecom SMA, as specified in this document, addresses four functional areas: Signaling, Media, QoS, and Security. These areas are described in the following sub-sections.

### 5.3.1 Signaling

IPCablecom SMA Signaling refers to the communication between the SMA gateway and the Event Server. This communication interface allows an MSO to control an SMA gateway and for the SMA gateway to respond to queries, and report required events.

To be able to communicate, the SMA gateway and the Event Server need to be aware of each other. The SMA gateway then needs to initiate communication with the Event Server and register to indicate its availability. Once registered, the SMA gateway can communicate any events generated by the SMA devices in the Home Domain. This also allows an Event Server to communicate MSO directives and information requests to the SMA gateway.

This interface is based on RESTful web services.

### 5.3.2 Media Session Establishment

Media in SMA may include both video and audio streams, also referred to as media sessions. Video sessions would generally be one way streaming video, although bidirectional video is permissible. Audio sessions may be either one-way or two-way. An example of a two-way audio stream would be a user pressing a panic button on an alarm panel and establishing a call to the central station.

---

Media session establishment uses the Session Description Protocol (SDP) and the Offer/Answer model, as specified in [RFC 4566] and [RFC 3264], respectively.

### 5.3.3 QoS

The Quality of Service for SMA is based on IP-Cablecom Multimedia defined in [TR-MM-ARCH]. The components that participate in QoS management in SMA take on the same behavior and have the same responsibilities as defined in the PCMM specifications. Please refer to [TR-MM-ARCH] for more information on how the CM, CMTS, and Policy Server components participate in QoS management.

The Event Server is responsible for identifying SMA requests that require QoS protection for packet flows that traverse the DOCSIS access network. The Event Server is also responsible for reserving, committing, and releasing QoS resources for all such flows.

The Application Manager serves as the interface between the IP-Cablecom SMA architecture and the IP-Cablecom Multimedia architecture. Its function is to receive QoS requests from the Event Server and to create and manage the IP-Cablecom Multimedia Gates for each flow using the COPS-based pkt-mm-3 interface.

The communication between the Event Server and the Application Manager is based on the IP-Cablecom Multimedia Web Service Interface Specification defined in [MM-WS]. The choice of a web service for this interface was made to allow for code reuse within the Event Server, which already has a RESTful web services interface for communication with the SMA gateway.

### 5.3.4 Security

SMA signaling contains potentially sensitive and personally identifiable information, such as status change events indicating conditions inside the house and instructions controlling SMA devices, such as alarm settings. Exposing the SMA signaling interface to unauthorized individuals may result in an unacceptable security risk. Specifically, without security, threats such as false event insertion, rogue instruction insertion, private data acquisition, and other common man-in-the-middle, denial of service, and replay attacks may be possible.

To mitigate such security threats, it is recommended that the SMA signaling be protected by a security mechanism to ensure the privacy of the communications as well as the authenticity and integrity of the data transmitted over the communications channel. While DOCSIS provides BPI+ as a mechanism for ensuring message privacy, authentication, and integrity, there are some situations in which relying on BPI+ may not be sufficient to address the security risks. For example, deployments which have turned off BPI+ security mechanism and deployments in which the SMA gateway resides on a customer's local area network which is not protected by BPI+, another security mechanism may be needed.

In keeping with the restful approach for SMA signaling, security in SMA is accomplished using Transport Layer Security (TLS), as specified in [RFC 4346] and [RFC 3268]. The usage of TLS for message encryption and message integrity is governed by configuration data. An SMA gateway may be configured to use TLS for all communication with its Event Server. The Event Server may be configured to only accept communication with a particular SMA gateway when that communication is protected by TLS. Some SMA gateways communicating with an Event Server may be required to use TLS while other SMA gateways communicating with the same Event Server may not be required to use TLS.

## 6 IPCABLECOM SMA SIGNALING INTERFACE REQUIREMENTS

IPCablecom SMA focuses primarily on the interactions between the SMA gateway and the Event Server, and any interfaces to support this communication. This specification describes the areas of Signaling, Media, QoS, and Security. The interfaces required to support this are illustrated in Figure 3.

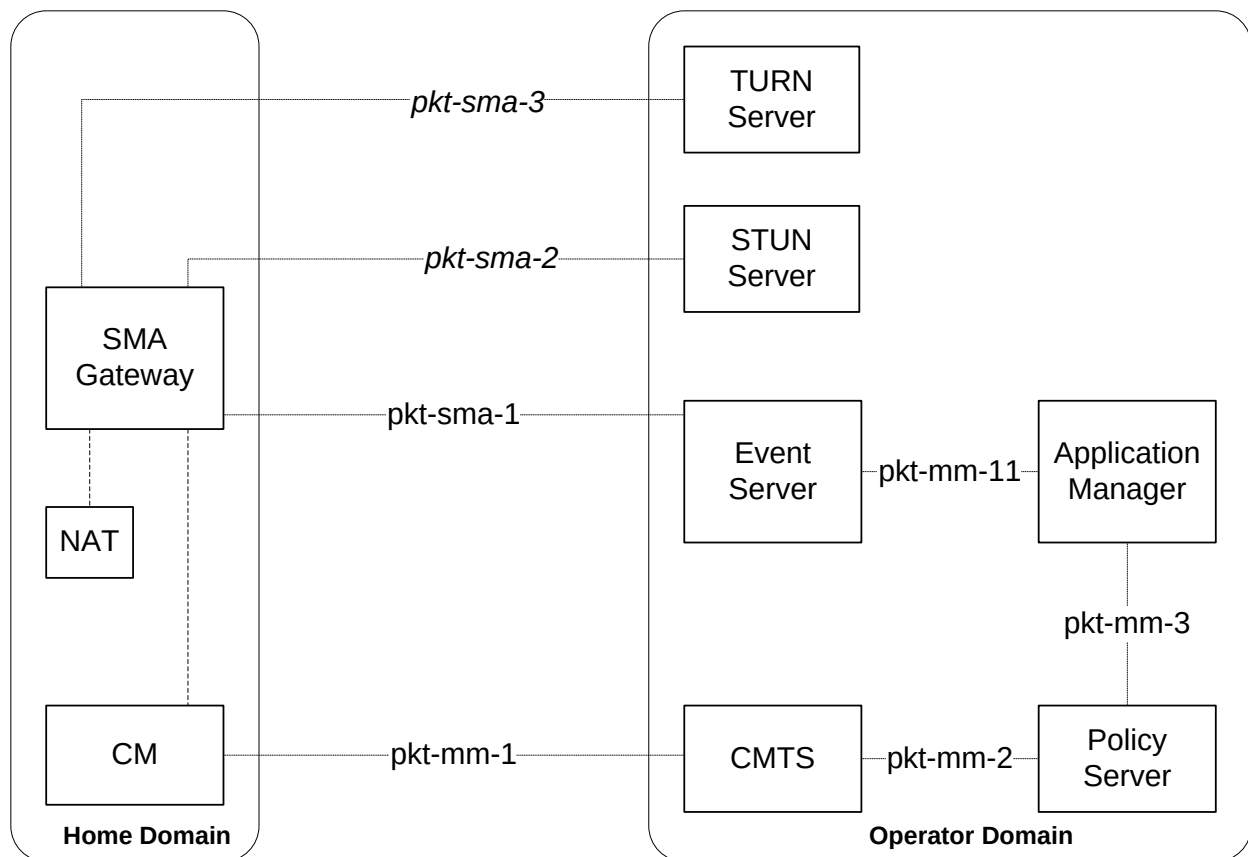


**Figure 3 - SMA Interfaces**

As shown in Figure 3, when the SMA gateway is connected via a DOCSIS Cable Modem, IPCablecom SMA reuses the IPCablecom Multimedia interfaces for QoS. It also specifies three interfaces: *pkt-sma-1*, *pkt-sma-2* and *pkt-sma-3*. The latter two are only required when the SMA gateway is connected via a NAT device, and hence are shown in italics. The functional areas addressed by these interfaces, and the interface requirements, are presented in the following sub-sections.

---

## 6.1 SMA Signaling

The SMA Signaling Interface is illustrated in Figure 4.

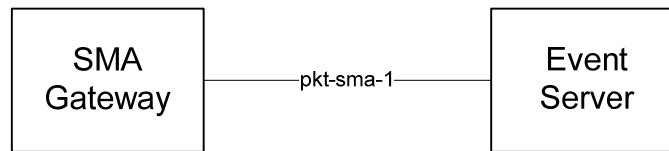


**Figure 4 - SMA Signaling Interface**

The interface, termed pkt-sma-1, allows for communication between the SMA gateway and the Event Server. The interface is realized via RESTful web services, which uses:

1. HTTP 1.1 ([RFC 2616]) as the communication protocol.
2. W3C XML 1.0 ([W3 XML1.0]) for data definitions, with the data models created using the W3C XML Schema Definition 1.0 ([W3 XSD1.0]).

This interface allows for the SMA gateway and the Event Server to send and receive SMA Messages. The requirements related to the HTTP protocol usage and URI formation, the SMA messages, error handling, and the backoff and retry mechanisms are specified in the following sub-sections.

### 6.1.1 HTTP Protocol Usage and URI Formation

This sub-section specifies the HTTP protocol usage and the HTTP URI formation. The following requirements apply:

- An SMA gateway implementing the pkt-sma-1 interface specified in this document **MUST** comply with the requirements specified in this sub-section.
- An Event Server implementing the pkt-sma-1 interface specified in this document **MUST** comply with the requirements specified in this sub-section.

The version of HTTP to be used for pkt-sma-1 **MUST** be HTTP 1.1, as specified in [RFC 2616]. The subset of possible HTTP operations that can be used for SMA messaging is limited to the following:

- GET
- POST
- PUT
- DELETE

The SMA gateway and the Event Server act as either the client or the server, based on the originator of an SMA message. When the SMA gateway is the originator of a message, it **MUST** use the following format for HTTP URI formation:

`http://<Event Server FQDN>/<resource ID>[(?<query string>)]`

When the Event Server is the originator of a message, it **MUST** use the following format for HTTP URI formation:

`http://<SMA gateway FQDN>/<resource ID>/[(?<query string>)]`

Where:

<Event Server FQDN > is the Event Server FQDN, provided during configuration.

---

<SMA gateway FQDN > is the identifier of the SMA gateway.

<resource ID> is the identifier for the resource.

<query string> additional filter criteria for a message type of 'instruction'.

The SMA gateway identifier (FQDN or URI) indicated above SHOULD include the Event Server Identifier. For example, if the Event Server FQDN is es.example.com, an SMA gateway that is connected to it should have an FQDN of sg.es.example.com. This will allow network elements that wish to establish communication with an SMA gateway (sg.es.example.com) to easily identify the Event Server through which a communication channel can be established (es.example.com).

Certain resource identifiers are reserved by this document. They are as follows:

- ALLKNOWNMADEVICES, refers to all the SMA devices known to an SMA gateway.
- ALLACTIVEMADEVICES, refers to the subset of all known SMA devices that are actively connected to an SMA gateway.
- ALLINACTIVEMADEVICES, refers to the subset of all known SMA devices that are not actively connected to an SMA gateway.
- <SMA Dev>/PROFILE, refers to the SMA device profile of the SMA device identified by <SMA Dev>.
- <SMA Dev>, refers to the current state of all the properties of the SMA device identified by <SMA Dev>.
- ev/<correlation ID | event ID, or HB>, refers to an event being generated, or the heartbeat.

When the SMA gateway related identifiers that refer to its connected SMA devices (above) are included in an instruction, the SMA gateway MUST return the applicable device identifiers, display names, namespaces, device tag (optional), schema locations (if the namespace is not a URI, or the URI does not indicate the Schema location) using the XML Schema specified in Annex A.6.

For the SMA device profile, refer to Annex A.9 and the example in Appendix III. This does not return the current state of the all properties. It returns the methods and properties supported by the specific device and related information such as property types, default values etc. When the SMA device is asked to return the current state of all the properties, the SMA device MUST return an SMA response (Annex A.5) that contains all the supported properties and their corresponding values.

### 6.1.2 SMA Messages

The messages exchanged between the SMA gateway and the Event Server are termed as SMA messages. This section provides more details regarding the SMA message types, message transmission, and their formats.

#### 6.1.2.1 Message Types

SMA messages can be categorized into two types: Instructions and Events. The Event Server can send across messages that control the state of the SMA services provided by the SMA gateway and the SMA network elements in the Home Domain. The SMA gateway can also send across a request to request the property on an Event Server (e.g., its registration state). Such SMA messages are termed instructions. A non-exhaustive list of instruction messages follows:

- Add SMA device: adds a new SMA device to the SMA gateway.
- Delete SMA device: removes a SMA device from the SMA gateway.
- Set Property: sets a SMA device property.

- 
- Get Property: gets a SMA device property.
  - Query Home Domain: returns the queried properties (e.g., connection status) for SMA devices that are connected to the SMA gateway in the home domain.
  - Create Logical Directive: a new directive (e.g., macros, triggers, schedules) is added.
  - Modify Logical Directive: a previously configured logical directive is updated.
  - Delete Logical Directive: removes a previously configured directive.

Messages can also be Events, which are messages that report the state of a particular entity or action on the originating entity. Events can be generated as a result of modification to SMA features, but they do not themselves modify the SMA features. They are transmitted from the SMA gateway to the Event Server and, optionally, the other way around. Examples of events include:

- SMA device connectivity, e.g., new SMA device found.
- SMA device state change: e.g., the motion sensor was triggered.

#### **6.1.2.2 Message Transmission**

Based on the RESTful web services approach for SMA signaling, each SMA message is transmitted via a HTTP method (e.g., HTTP GET). The HTTP method identifies the intent:

- The HTTP GET operation is used to transmit an instruction to retrieve a resource. A resource can be one or more properties, or property fields, within an Event Server, SMA gateway, or an SMA device. For example, the instruction can request a list of all SMA devices connected to an SMA gateway.
- The HTTP POST operation is used to identify an SMA Message instruction or an event. An example of an instruction is media session establishment. An example of an event is triggering of a sensor.
- The HTTP PUT operation is used to identify an instruction to modify the contents of a resource. For instance, the Event Server can instruct the SMA gateway to modify the contents of a specific resource or property. It is to be noted that such a resource already exist. For creation, a HTTP POST operation is used.
- The HTTP DELETE operation identifies an instruction to delete a specific resource. For example, the SMA gateway may be instructed to delete a connected SMA device.

The following requirements apply to the SMA gateway:

- The SMA gateway **MUST** support the HTTP methods - GET, POST, PUT, DELETE - as specified in this document. As a note, while the SMA gateway can receive a HTTP DELETE request, the SMA gateway **MUST NOT** use the HTTP DELETE operation when it communicates with the Event Server.
- Upon receiving a HTTP request from the SMA gateway, the Event Server **MUST** respond immediately with a suitable HTTP response (e.g., 200 OK). It is to be noted that if the HTTP method contains an instruction, the HTTP response may or may not contain an SMA response as specified later in this section.

The following requirements apply to the Event Server:

- The Event Server **MUST** support the HTTP methods - GET, POST, PUT and DELETE - as specified in this document.
- An Event Server that receives a HTTP DELETE operation from the SMA gateway **MUST** reject the request with a HTTP 403 response.
- Upon receiving a HTTP request from the SMA gateway, the Event Server **MUST** respond immediately with a suitable HTTP response (e.g., 200 OK). It is to be noted that when the HTTP method contains an instruction, the HTTP response may or may not contain an SMA response as specified later in this section.