SES

SAT>IP™

Operator Extensions

Version 0.9.4

Author	Date	Version	Comment
SES S.A.	04.09.2015	0.9.4	

Table of Contents

Acronyms

CA	Conditional Access
CAM	Conditional Access Module
CSV	Comma Separated Values
DHCP	Dynamic Host Configuration Protocol
DiSEqC	Digital Satellite Equipment Control
DLNA	Digital Living Network Alliance
DSL	Digital Subscriber Line
DVB	Digital Video Broadcasting
DVB-S	DVB for Satellite
DVR	Digital Video Recorder
FEC	Forward Error Correction
FTA	Free-To-Air
GENA	General Event Notification Architecture
HTML	HyperText Markup Language
HTTP	Hyper Text Transfer Protocol
HSPA	High Speed Packet Access
IF	Intermediate Frequency
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LAN	Local Area Network
LNB	Low Noise Block
MDU	Multi Dwelling Unit
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MPTS	Multiple Program Transport Stream
MUDP	Multicast UDP
NAS	Network Attached Storage
PLC	Power Line Communication
PoE	Power over Ethernet
PSK	Phase Shift Keying
PVR	Personal Video Recorder
QPSK	Quaternary Phase Shift Keying
RFC	Request For Comments
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
RTSP	Real Time Streaming Protocol
SDES	Source Description
SDP	Session Description Protocol
SI	Service Information
SMATV	Satellite Master Antenna Television
SOAP	Simple Object Access Protocol
SPTS	Single Program Transport Stream
SR	Sender Report
SSDP	Simple Service Discovery Protocol
STB	Set-Top-Box
TCP	Transport Control Protocol
TS	Transport Stream
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
UPnP AV	UPnP Audio and Video
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF	UCS Transformation Format
WLAN	Wireless LAN
XML	Extensible Markup Language

References

SAT>IP

[1] SAT>IP Protocol Specification

Scrambling Specification

[2] FIPS-197: Federal Information Processing Standards (FIPS) Publication 197, Specification for the Advanced Encryption Standard (AES), November 2001

[3] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001

[4] ATIS-0800006 IIF Default Scrambling Algorithm (IDSA), IPTV Interoperability Specification

Audio and Video

[5] Recommendation ITU-T H.222.0 / ISO/IEC 13818-1:2013: "Information technology - Generic Coding of moving pictures and associated audio information: Systems", ITU-T Recommendation H.222.0 (2012)/Amendment 3 / ISO/IEC 13818-1:2013/Amd3:2014: "Transport of HEVC video over MPEG-2 Systems"

[6] ITU T Rec. H.262 | ISO/IEC 13818-2 (2nd edition, 2000): "Information Technology - Generic Coding of moving pictures and associated audio: Video"

[7] ITU T Rec. H.264 | ISO/IEC 14496 10 AVC: "Advanced Video Coding for Generic Audiovisual Services", May 2003 / ISO/IEC 14496-10:2004/AM 1, Part 10: Advanced Video Coding AMENDMENT 1: AVC fidelity range extensions

[8] Recommendation ITU-T H.265 | ISO/IEC 23008-2:2013: "Information technology - High efficiency coding and media delivery in heterogeneous environments - Part 2: High efficiency video coding".

[9] ISO/IEC 11172-3 (1993): "Information Technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s - Part 3: Audio"

[10] ISO/IEC 14496-3:2009: "Information technology -- Coding of audio-visual objects -- Part 3: Audio".

[11] ETSI TS 102 366: "Digital Audio Compression (AC-3, Enhanced AC-3) Standard".

1 Introduction

This document provides two extensions to the core SAT>IP Specification. These extensions are mainly for deployment in operator scenarios. The first extension concerns transcoding of video and audio services and the second one transcrypting of services from standard DVB Conditional Access (CA) towards common Digital Rights Management (DRM) technologies. An operator can use one or both extensions in his device as required.

1.1 Usage Scenario

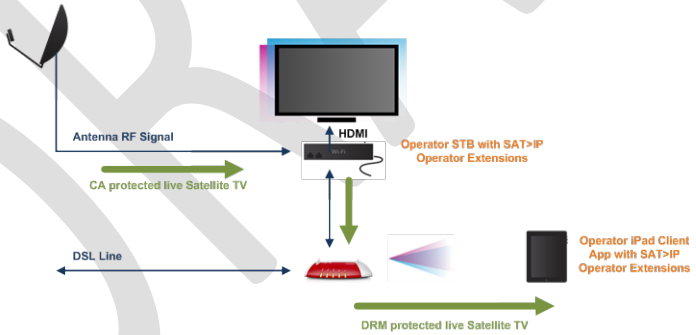
The SAT>IP Operator Extensions are normally implemented in Operator Set-Top-Boxes or Operator Gateways. They can be used in conjunction with traditional or standard SAT>IP based signal distribution topologies.

SAT>IP Clients implementing the Operator Extensions are always capable of receiving FTA programs also from standard SAT>IP servers that do not implement the Operator Extensions.

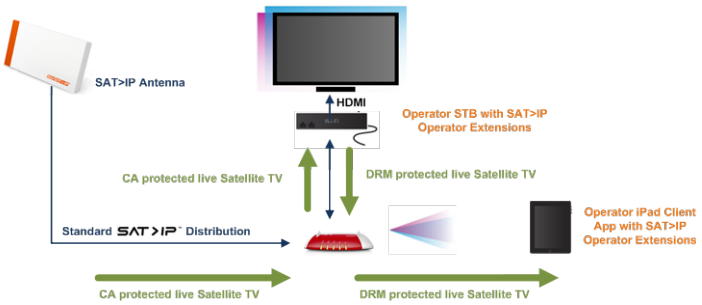
SAT>IP Servers implementing the Operator Extensions are capable of co-existing on the local network with standard SAT>IP servers that do not implement the Operator Extensions.

SAT>IP Servers implementing the Operator Extensions can be connected to the satellite antenna directly via RF or alternatively can act themselves as SAT>IP Clients in order to source signals from another SAT>IP Server which may e.g. be part of the antenna (IP-LNB or SAT>IP Flat Antenna). Both cases are illustrated below:

1.1.1 RF based topology



1.1.2 SAT>IP based signal distribution



2 Transcoding

2.1 Introduction

Existing SAT>IP Clients do not expect a certain bitrate or codec to be delivered to them. They only request certain PIDs from certain transponders to be forwarded.

Thus standard SAT>IP servers (not corresponding to these extensions) can already apply transcoding when forwarding satellite received signals to clients. As the transcoding decision will have to be taken by the server we call this server-driven transcoding.

These extensions add a second option for handling transcoding. This option will be described in this chapter and can be considered as a client-driven transcoding solution. The client decides to request from the server a particular media stream by specifying a particular codec and bitrate to be used.

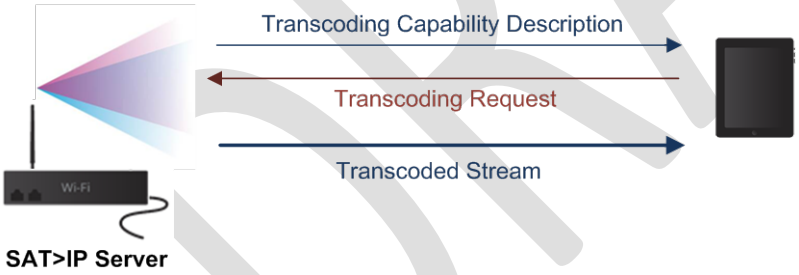
In neither of these schemes do we specify how a client or a server takes a transcoding decision or how the client or server estimates the best possible bitrate or codec.

Please note:

Transcoding always deteriorates the original video signal quality and after a transcoding process the video quality cannot be superior to the original. The recommendation is therefore to apply transcoding carefully and only in situations where transparent operation is not possible.

Client driven transcoding involves two core mechanisms:

- A possibility for servers to announce the supported codec capabilities
- A mechanism for clients to request a media stream according to specific parameters



2.2 Transcoding Capability Description

SAT>IP Servers supporting transcoding shall add a capabilities element to the XML description of Section 3.4 in [1].

A **<satip:X_SATIPTRC>** capabilities element should be included in the XML description of a SAT>IP server in order to indicate to clients which video and audio codecs the server supports together with a minimum and maximum bitrate for each codec.

This additional XML element shall be put at the end of the <device> elements in the XML Device Description.

The value of the <satip:X_SATIPTRC> element is a comma separated variable length list.

The values (of which there maybe a variable number) are composed each of a coder name followed by the “@” sign, followed by a minimum and maximum bitrate supported by that coder. The end of the list contains the container formats available. The container formats do not contain the “@”sign.

Example of a SAT>IP server including one or more transcoders that support AVC for bitrates ranging from 2Mbit/s to 8 Mbit/s, HEVC for bitrates ranging from 1 to 4 Mbit/s and AAC-LC transcoders that support audio rates from 10kbit/s to 320 kbit/s within the supported container format TS.

```
<satip:X_SATIPTRC xmlns:satip="urn:ses-com:satip">avc@2M:8M,hevc@1M:4M,lcaac@10K:320K,ts</satip:X_SATIPTRC>
```

Syntax:

The namespace for <satip:X_SATIPTRC> must be "urn:ses-com:satip" and the namespace prefix must be "satip:".

Supported Transcoder Values:

	Value	Profile
Video	avc	HP@L4
	hevc	MP@L4.1 Main Tier
Audio	lcaac	
	heaac	HE-AAC v1
Container	ts	MPEG-2 TS

Table 2.2.1

Profile, Level and Tier definitions are according to Ref[6-11].

Framerates

Transcoding in SAT>IP never changes the framerate. The output framerate is always equal to the input framerate.

Supported Bitrates

Bitrates consist each of a minimum value followed by a maximum value. Both values are separated by a colon sign. M denotes Mbit/s and K denotes Kbit/s.

The container format is not followed by a bitrate.

Example Values:

```
avc@2M:8M
hevc@1M:4M
lcaac@10K:320K
ts
```

Example Description File

```
<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0" configId="0">
  <specVersion>
    <major>1</major>
    <minor>1</minor>
  </specVersion>
  <device>
    <deviceType>urn:ses-com:device:SatIPServer:1</deviceType>
    <friendlyName>SATIPBOX</friendlyName>
    <manufacturer>Manufacturer</manufacturer>
    <manufacturerURL>http://www.manufacturer.com</manufacturerURL>
    <modelDescription>SATIPBOX 500 4.0</modelDescription>
    <modelName>SATIPBOX</modelName>
    <modelNumber>1.0</modelNumber>
    <modelURL>http://www.manufacturer.com/satipbox</modelURL>
    <serialNumber>1S81A31231000007</serialNumber>
    <UDN>uuid:50c958a8-e839-4b96-b7ae-8f9d989e136c</UDN>
    <iconList>
      <icon>
        <mimetype>image/png</mimetype>
        <width>48</width>
        <height>48</height>
        <depth>24</depth>
        <url>/icons/sm.png</url>
      </icon>
      <icon>
        <mimetype>image/png</mimetype>
        <width>120</width>
        <height>120</height>
        <depth>24</depth>
        <url>/icons/lr.png</url>
      </icon>
      <icon>
        <mimetype>image/jpeg</mimetype>
        <width>48</width>
        <height>48</height>
        <depth>24</depth>
        <url>/icons/sm.jpg</url>
      </icon>
      <icon>
        <mimetype>image/jpeg</mimetype>
        <width>120</width>
        <height>120</height>
        <depth>24</depth>
        <url>/icons/lr.jpg</url>
      </icon>
    </iconList>
    <presentationURL>/index.htm</presentationURL>
    <satip:X_SATIPCAP xmlns:satip="urn:ses-com:satip">DVBS2-8,DVBT-4</satip:X_SATIPCAP>
    <satip:X_SATIPM3U xmlns:satip="urn:ses-com:satip">/channellist.m3u</satip:X_SATIPM3U>
    <satip:X_SATIPTRC xmlns:satip="urn:ses-com:satip">avc@2M:8M,hevc@1M:4M,lcaac@10K:320K,ts</satip:X_SATIPTRC>
  </device>
</root>
```

2.3 Transcoding Query Syntax Extensions

SAT>IP Clients, according to these extensions, may send standard SAT>IP queries as defined in [1] to SAT>IP servers.

In addition SAT>IP Clients, according to these extensions, may add a specific query attribute if they wish to receive the satellite delivered streams not in their original codec and bitrate but rather transcoded to a different video and/or audio codec.

The additional query attribute parameters required for describing a transcoding request are provided below:

Name	Attribute	Values	Example
Transcoding Parameters	trcd	CSV list of parameters: Target Video codec Set to one of the following values: “avc”, “hevc”. Target Video bitrate Numerical value between 1 and 1000 followed by M for Mbit/s or K for kbit/s The video bitrate corresponds to the peak rate that the client is prepared to accept. The actual bitrate is dependent on the encoder implementation. Target Video format One of the following values: “1080P”,”1080i”,”720P”,”576P”,”576i”,”288P”,”144P”. These values correspond to the following horizontal and vertical resolutions:	**`trcd=avc,800K,720,aac,128K,ts`** **`trcd=avc,800K,720,,,ts`**

Value	Horizontal Resolution	Vertical Resolution
1080P 1080i	1920	1080
720P	1280	720
576P 576i	720	576
288P	352	288
144P	176	144

“P” or “i” indicate whether the target output video format should be Progressive or interlaced.

Target Audio codec
Set to one of the following values: “mp2”, “lcaac”, “heaac”.
Target Audio bitrate
Numerical value between 1 and 320 followed by K for kbit/s.
The server shall set the audio transcoder to this value. The actual bitrate may depend on the encoder implementation. The rate corresponds to the value for a single stereo pair.
Target Container Format
The only allowed value for this attribute is “ts”.

The trcd attribute shall always list at least all the video related parameters (see examples above). When audio transcoding is not required the audio transcoding values may be left empty (see example 2 above).

The trcd attribute shall never be empty. If no transcoding is requested the trcd attribute shall not be present in the query.

If transcoding is requested, the dvbtrp attribute must also be present in the query. The dvbtrp attribute is specified in section 3.3.3

Example Transcoding Query:

rtsp://192.168.1.202/?src=1&freq=12604&pol=h&msys=dvbs&mtype=qpsk&sr=22000&fec=56&pids=0,1290,2290,7290&trcd=avc,800K,720,aac,128K,ts&dvbtrp=1,1019,10301

2.4 PSI/SI Usage and Adaptations for Transcoded Services

SAT>IP servers that are capable of video and/or audio transcoding also need to be able to adapt the PSI / SI information for the services that are being transcoded. When transcoding is active, the following rules shall be applied:

- The SAT>IP server shall receive and parse the original PAT. .
- The server shall parse the PAT to extract the PID of the PMT of the service which is identified by the service ID provided in the dvbtrp attribute.
- The SAT>IP server shall receive and parse the original PMT. The SAT>IP server shall monitor the PAT and PMT for version updates.
- If PID 0 is requested from a SAT>IP client, the SAT>IP server shall stream the PAT of the requested transponder.
- If the PMT PID of the selected service is requested from a SAT>IP client, a transcoded PMT shall be streamed by the SAT>IP server (see below for the definition of the transcoded PMT).
- If a requested PID is listed in the PMT of the selected service and the PID is an audio stream and audio transcoding is requested, the transcoded audio stream as defined by the audio transcoding attributes shall be provided to the client. If no audio transcoding is requested, the original audio stream shall be provided.
- If a requested PID is listed in the PMT of the selected service and the PID is a video stream, the transcoded video stream as defined by the video transcoding attributes shall be provided to the client.
- If a requested PID is listed in the PMT of the selected service but is not an audio or video stream, the unchanged PID shall be passed to the client.
- If a requested PID is the PCR PID of the selected service, this PCR PID shall be streamed to the client.

In all other cases the PIDs shall be streamed unchanged.

No more than one audio PID and one video PID shall be requested at the same time. This means that the server never needs to transcode more than one audio and video stream at the same time.

MPTS are not supported. Therefore, "pids=all" shall not be used in the RTSP query.

PMT Transcoding rules:

The transcoded PMT is generated from the original PMT as follows:

The transcoded PMT contains the same PIDs in the same order as the original PMT.

The PCR PID of the transcoded PMT may be different of the PCR PID as defined in the original PMT. Using a different PCR PID may be necessary due to restrictions of the transcoder hardware of the SAT>IP server device. In this case the SAT>IP server shall automatically select a new unused PID for PCR.

If audio transcoding is used, all audio components of the PMT shall be updated to reflect the target audio codec as defined by the audio transcoding.

If video transcoding is used, all video components of the PMT are updated to reflect the target video codec as defined by the video transcoding.

All other PIDs of the original PMT are used unchanged in the transcoded PMT.

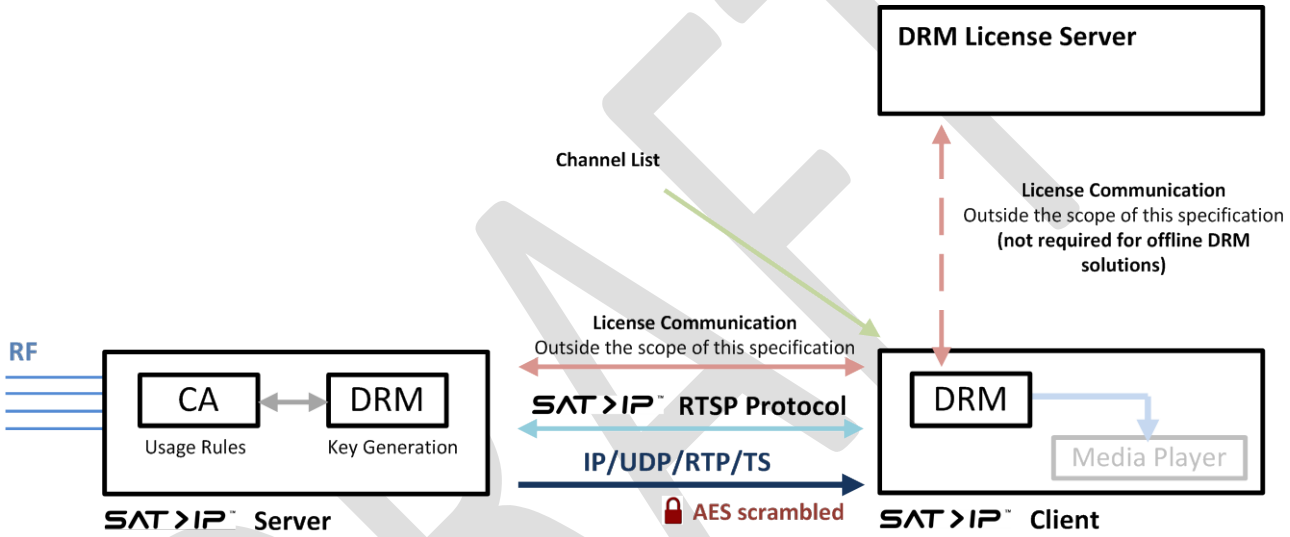
3 Transcrypting

3.1 Introduction

SAT>IP Servers that implement these extensions are capable of protecting an incoming stream (FTA or CA) with an additional Digital Rights Management layer. The purpose of the Digital Rights Management Scheme is to control the forwarding of signals only to trusted devices.

This mode of operation is required by Pay-TV Operators in order to protect access to their content when such access is granted outside the traditional Conditional Access environments e.g. when accessing high-value content on tablets or PCs.

The following illustration shows how a DRM system integrates with SAT>IP.



DRM Support in SAT>IP allows servers to announce their DRM support to clients and allows clients to decide whether the DRMs supported are sufficient to setup a DRM protected connection with the server in order to stream content.

3.2 Transcrypting Capability Description

A SAT>IP server announces its content protection capabilities through the Device Description Document.

A <satip:X_SATIPCPT> capabilities element shall be included in the XML description of a SAT>IP server for each DRM or Link Protection scheme that the server supports.

This(these) additional XML element(s) shall be put at the end of the <device> elements in the XML Device Description.

The namespace for <satip:X_SATIPCPT> must be "urn:ses-com:satip" and the namespace prefix must be "satip:".

Syntax:

The value of the <satip:X_SATIPCPT> element is a comma separated list with the following arguments:

Arguments
Content Protection Scheme,
Operator Name,
Profile,
Version,
Area,
Operator Specific Text Field,
DRM or LP System,
DRM or LP Version,
Scrambling Algorithm

Table 3.2.1

Example:

Example of a server that supports HD+ Multiroom using NagraPRM with the standard AES-ATIS scrambler of SAT>IP.

```
<satip:X_SATIPCPT xmlns:satip="urn:ses-com:satip">CA2DRM,HD+,Multiroom,1.0,Germany,free_text_field,NPRM,1.0,AES-ATIS</satip:X_SATIPCPT>
```

The Argument values are defined below:

The Content Protection Schemes that are currently defined are:

Value	Name
CA2DRM	For SAT>IP Servers implementing a full CA to DRM solution
LP	For SAT>IP Servers implementing the standard Link Protection scheme of SAT>IP

Table 3.2.2

The Operator Name field contains the name of the platform operator:

Value	Name
HD+	HD Plus GmbH Germany

Table 3.2.3

The Profile is an operator specific text field (max 32 characters).

The Version corresponds to the version of the profile. It contains major and minor version numbers separated by a dot. Example: 1.2

The Area field is an operator specific field that can be used to signal a geographic target area.

The Operator Specific Text Field field is another field that the operator can use to signal proprietary information (max 64 characters).

The DRM or LP System can take one of the values below to describe the actual DRM or Link Protection system implemented on the SAT>IP server device:

Value	Name
NPRM	Nagra PRM

Table 3.2.4

The DRM or LP Version number corresponds to the version of the DRM or LP solution. It contains major and minor version numbers separated by a dot. Example: 1.2.

The Scrambling Algorithm can take one of the values below:

Value	Scrambling Algorithm
AES-ATIS	AES ATIS

Table 3.2.5

If a SAT>IP server supports more than one DRM or LP scheme, an additional <satip:X_SATIPCPT> capabilities element shall be included in the XML description of a SAT>IP server for each system supported.

It is the client's responsibility to request the DRM protection that it supports.

3.3 DRM Operation

3.3.1 Introduction

SAT>IP Clients request content from SAT>IP servers. SAT>IP servers always forward content transparently. This means that CA protected content is always forwarded transparently and unchanged (remains encrypted).

DVB Services which are protected by a Conditional Access Scheme can only be forwarded unencrypted if – the SAT>IP server has the necessary credentials (CA+smartcard+rights), - the usage rules allow the CA kernel to do this and - upon explicit request by the client.

The SAT>IP Client learns about the encryption status of the signal and the corresponding usage rules by analysing the Service information and Program Specific Information carried in the DVB Transport Stream or by being informed about this via the client application backend if available.

The SAT>IP Client thereupon triggers the transcryption to DRM and forwarding of the signal by sending an extended transcryption query as described in chapter 3.5.

The DRM license acquisition process between SAT>IP DRM client and SAT>IP DRM server as well as between SAT>IP DRM client and Backend License Server is outside the scope of this specification. Such communication shall not interfere with the RTSP session mechanism of SAT>IP and can run in parallel to it. It is recommended to base such license related communication on http or https.

3.3.2 License Acquisition

All communication related to license acquisition is outside the scope of this specification as it is specific to the actual DRM solution being used.

3.3.3 Transcrypting Query Syntax Extensions

A SAT>IP client indicates to the SAT>IP server that it requests a particular stream to be DRM protected by adding the following attribute to a standard SAT>IP request.

cdrm=Content Protection Scheme,Operator Name,Profile,Version,DRM or LP System,DRM or LP Version,Scrambling Algorithm

Name	Attribute	Value	Examples
		Range	
Transcrypting Parameters	cdrm	CSV list of parameters: Content Protection Scheme Set to one of the values of Table 3.2.2 Operator Name Set to one of the values of Table 3.2.3 Profile Set to the corresponding value of the SATIPCPT element Version Set to the corresponding value of the SATIPCPT element DRM or LP System Set to one of the values of Table 3.2.4 DRM or LP Version The Version Number corresponds to the version of the DRM solution. It contains the major and minor version numbers separated by a dot. The version number needs to fit the version number in the XML capabilities element Scrambling Algorithm Set to one of the values of Table 3.2.5	**`cdrm=NPRM,1.0,AES-ATIS`**

Example of a transcrypting request:

rtsp://192.168.1.202/?src=1&freq=12604&pol=h&msys=dvbs&mtype=qpsk&sr=22000&fec=56&pids=0,1290,2290,7290&
cdrm=CA2DRM,HD+,Multiroom,1.0,NPRM,1.0,AES-ATIS

Some CA implementations require DVB triplet information to be provided by the client in addition to the physical tuning parameters. For this purpose an additional attribute is defined in these extensions.

dvbtrp=Original Network ID,Transport Stream ID,Service ID

Name	Attribute	Value	Examples
		Range	
DVB Triplet	dvbtrp	CSV list of parameters: Original Network ID (ONID) Decimal value between 0 and 65535 Transport Stream ID Decimal value between 0 and 65535 Service ID Decimal value between 0 and 65535	**`dvbtrp=1,1019,10301`**

Example of a request including the DVB Triplet:

rtsp://192.168.1.202/?src=1&freq=12604&pol=h&msys=dvbs&mtype=qpsk&sr=22000&fec=56&pids=0,1290,2290,7290&
cdrm=CA2DRM,HD+,Multiroom,1.0,NPRM,1.0,AES-ATIS&dvbtrp=1,1019,10301

3.4 PSI/SI Usage and Adaptations for Transcrypted Services

When transcrypting is active, the following rules shall be applied:

- The SAT>IP server shall receive and parse the original PAT from the broadcast stream.

- The server shall parse the PAT to extract the PID of the PMT of the service which is identified by the service ID provided in the dvbtrp attribute.

- The SAT>IP server shall receive and parse the original PMT.

- The SAT>IP server shall monitor the PAT and PMT for version updates.

- If PID 0 is requested from a SAT>IP client, the SAT>IP server shall stream the unecrypted PAT of the tuned transponder.

- If the PMT PID of the selected service is requested from a SAT>IP client, the unencryted PMT shall be streamed by the SAT>IP server.

- If a requested PID is listed in the PMT of the selected service and the PID is an audio stream, the transcrypted audio stream shall be provided.

- If a requested PID is listed in the PMT of the selected service and the PID is an video stream, the transcrypted video stream shall be provided.

- If a requested PID is listed in the PMT of the selected service but is not an audio or video stream, the unchanged unencrypted PID shall be passed to the client.

- If a requested PID is the PCR PID of the selected service, this PCR PID shall be streamed to the client. The PCR PID may or may not be the same as one of the video or audio streams.

- In all other cases the PID shall be streamed unchanged.

- MPTS are not supported. Therefore, "pids=all" shall not be used in the RTSP query.

3.5 CA related error messages

CA related error messages can be provided by the server using standard server error response messages: e.g. Error 503 “Service Unavailable”.

The message body of the response may contain the “CA-Message:” parameter followed by a textual description of the error e.g. “No smartcard present” or “Access rights expired”

3.6 Scrambling Algorithm

This specification describes a prefered DRM scrambling algorithm to be used by all SAT>IP Servers and Clients that implement these extensions. The use of a common scrambling algorithm allows SAT>IP server sourced streams to be provided to various types of SAT>IP clients and provides a certain level of interoperability in the presence of different DRM Key Management solutions.

3.6.1 AES (ATIS)

The core scrambling algorithm used in the SAT>IP Operator Extensions is based upon the Advanced Encryption Standard (AES). AES is a well-reviewed, widely-accepted cryptographic algorithm that has had a thorough and expert design review to ensure its cryptographic robustness.

By selecting a single scrambling algorithm the same server sourced streams could be made use of under different DRM solutions if required. (simulcrypt-like operation)

Base Algorithm: **AES**
This is a publicly available cryptographic algorithm that has been standardized by the NIST as DIPS-197 [2].

Key Length: **128 bits**
128 bits is deemed sufficient to protect content from plausible threats.

Mode: **CBC** (Cipher Block Chaining).
CBC is one of several standardized modes in [3].

Only the Payload of the MPEG-2 Transport Stream Packets is scrambled, the Header and the optional Adaptation Fields are not scrambled.

All the details related to the implementation of this mode in the context of MPEG Transport Streams are clearly described in the ATIS document 0800006 [4]**.** ATIS refers to this design as IDSA (IPTV Default Scrambling Algorithm).

The ATIS implementation was designed with the intent to produce a license and patent free solution.

The algorithm selected is both Software and Hardware Friendly.

The use of the above scrambling algorithm does not preclude that some operators may select to use a different Scrambling Algorithm for commercial reasons.

4 IP Link Protection

In addition to the implementation of a full CA to DRM transcoding solution, these Extensions also offer a way of protecting the IP link between a SAT>IP server and a SAT>IP Client through a common lightweight link protection scheme.

This scheme has the potential to become part of standard SAT>IP Client implementations and can ideally work across different operator platforms.

TBA