

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.290

(11/2006)

SERIES J: CABLE NETWORKS AND TRANSMISSION
OF TELEVISION, SOUND PROGRAMME AND OTHER
MULTIMEDIA SIGNALS

Cable modems

Next generation set-top box core architecture

ITU-T Recommendation J.290



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T Recommendation J.290

Next generation set-top box core architecture

Summary

This Recommendation describes a core architecture functionality of next-generation STB that operators and equipment vendors MAY elect to follow in making network and product investment decisions. This architecture defines a cost-efficient platform with capacity and flexibility to support growth of on-demand video, high definition digital TV, managed in-home networks connecting a wide range of consumer-provided devices, and future IP multimedia services including IP voice, video telephony, and multiplayer gaming. The goal of this Recommendation is to provide core functionalities and can serve as foundations for network specific environments. It SHOULD be noted that home networking portion of this architecture is based upon ITU-T Rec. J.190. In actual implementation of NG-STB-A functionalities, this Recommendation MUST be used with either ITU-T Rec. J.292 or ITU-T Rec. J.291 based on access network availability.

Source

ITU-T Recommendation J.290 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2007

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
4	Abbreviations and acronyms	2
5	Conventions	5
6	Integrated multimedia architecture	5
6.1	Reference architecture description	6
6.2	Attributes of an integrated multimedia architecture	7
6.3	Video services architecture.....	9
6.4	IP multimedia services architecture.....	17
6.5	In-home network architecture.....	20
6.6	Advanced digital advertizing.....	28
7	Customer premises.....	28
7.1	Overview	28
7.2	Subscriber video devices (SVDs).....	29
7.3	Other CPE devices.....	33
8	Security	34
8.1	Security hardware element	34
8.2	Authentication	34
8.3	Key encryption keys	34
8.4	Unit address	34
8.5	Tamper resistance	35
8.6	Key management	35
8.7	Copy protection	36
9	Head-end network architecture.....	36
9.1	Head-end network delivery architecture	37
9.2	Session and resource management architecture	38
10	Quality of service.....	39
10.1	IntServ and DiffServ.....	40
10.2	End-to-end QoS and service applications.....	40
10.3	Requirements for QoS bridge.....	41
	Appendix I – Relationship between MI and cable type services and QoS type	45
	Bibliography.....	46

ITU-T Recommendation J.290

Next generation set-top box core architecture

1 Scope

This Recommendation describes a core architecture functionality of next-generation STB that operators and equipment vendors MAY elect to follow in making network and product investment decisions. This architecture defines a cost-efficient platform with capacity and flexibility to support growth of on-demand video, high definition digital TV, managed in-home networks connecting a wide range of consumer-provided devices, and future IP multimedia services including IP voice, video telephony, and multiplayer gaming. The goal of this Recommendation is to provide core functionalities and can serve as foundations for network specific environments. It SHOULD be noted that home networking portion of this architecture is based upon ITU-T Rec. J.190. In actual implementation of NG-STB-A functionalities, this Recommendation MUST be used with either ITU-T Rec. J.292 or ITU-T Rec. J.291 based on access network availability.

2 References

None.

3 Definitions

This Recommendation defines the following terms:

3.1 authorized service domain (ASD): The devices in this domain are able to authenticate themselves and support content usage rights as defined by the network operator.

3.2 application ID: This is a field indicating a numeric ID for an application running on the set-top device.

3.3 authorized output domain (AOD): The devices in this domain are connected to the ASD using operator-approved output interfaces.

3.4 best effort domain (BED): Devices and physical layer segments not conforming to the requirements of ASD, AOD, GSD. The devices in this domain do not require content protection or guaranteed quality of service.

3.5 CA_system_ID: This is a field indicating the type of CA system applicable for either the associated ECM and/or EMM streams. The CA_system_ID may be used as a DSG client ID in DSG advanced mode.

3.6 DSG client: The DSG (DOCSIS set-top gateway) client terminates the DSG tunnel and receives content from the DSG server.

3.7 entitlement control messages (ECMs): An ECM is an encrypted message that contains access criteria to various service tiers and a control word (CW).

3.8 embedded PS: A portal services element that does not use a stand-alone interface to connect to a set-top box device.

3.9 embedded set-top box: An embedded set-top box is an embedded service application functional entity. It includes the DSG client(s), a DSG client controller, an embedded processor for an application environment, and either an embedded or removable module for conditional access.

3.10 entitlement management messages (EMMs): The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device.

- 3.11 guaranteed service domain (GSD):** Devices in the GSD will be able to receive QoS-sensitive content services such as VoIP, multiplayer interactive gaming, and IP video-phone.
- 3.12 home access (HA) device:** A grouping of logical elements used to achieve HFC access for IP-Cable2Home network(s).
- 3.13 home bridge (HB) device:** A group of logical elements used to bridge IP-Cable2Home networks together.
- 3.14 home client (HC) device:** A group of logical elements used to provide functionality to client applications.
- 3.15 LAN IP device:** A LAN IP device is representative of a typical IP device expected to reside on home networks, and is assumed to contain a TCP/IP stack as well as a DHCP client.
- 3.16 portal services (PS):** A functional element that provides management and translation functions between the HFC and home network.
- 3.17 one-way:** This expression infers that the downstream path (from the network to the subscriber) is operational, and that the upstream path (from the subscriber to the network) is not operational. This may occur because the upstream path is not available, the set-top device is not registered, or the set-top device does not support a two-way mode of operation.
- 3.18 QoS parameter set:** The set of service flow encodings that describe the quality of service attributes of a service flow or a service class.
- 3.19 residential gateway:** The device that provides interconnection functionalities between access network and home network as described in ITU-T Rec. J.190.
- NOTE – How to apply J.190 residential gateway functionality to various networks SHOULD be considered in the near future.
- 3.20 service class:** A set of queuing and scheduling attributes that is named and that is configured at the head-end equipment. A service class is identified by a service class name. A service class has an associated QoS parameter set.
- 3.21 set-top controller:** This is the computer system responsible for managing the set-top devices within a cable system. It manages set-top devices through control and information messages sent via the out-of-band channel.
- 3.22 set-top device:** A receiver that contains an embedded PS function for home network connectivity and an embedded set-top box.
- 3.23 two-way:** This expression infers that the downstream path and the upstream path are operational.
- 3.24 well-known MAC address:** This refers to the MAC address of the client within the set-top device. This MAC address has been assigned by the manufacturer of the conditional access system within the set-top device.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
API	Application Programming Interface
ASD	Authorized Service Domain
BED	Best Effort Domain
BP	(IP-Cable2Home) Boundary Point

CA	Conditional Access
CAS	Conditional Access System
CBC	Cipher Block Chaining
CE	Consumer Electronics
CMTS	Cable Modem Termination System
Codec	Coder/Decoder
CPE	Customer Premises Equipment
CSA	Common Scrambling Algorithm
CSP	Configurable Security Processor
CW	Control Word
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services Architecture for Network Traffic
DLNA	Digital Living Network Alliance
DRM	Digital Rights Management
DSCP	DiffServ Code Point
DSL	Digital Subscriber Line
DTCP	Digital Transmission Content Protection
DTV	Digital TV
DVB	Digital Video Broadcast
DVI	Digital Video Interface
DVR	Digital Video Recording
ECB	Electronic Code Book
ECM	Entitlement Control Message
EMM	Entitlement Management Message
EPG	Electronic Program Guide
FIPS	Federal Information Processing Standards
FTTH	Fibre to the Home
GigE	Gigabit Ethernet
GSD	Guaranteed Service Domain
HDCP	High-bandwidth Digital Content Protection
HDMI	High Definition Multimedia Interface
HDTV	High Definition TV
HFC	Hybrid Fibre Coaxial
ID	Identifier
IP	Internet Protocol
Layer 3	Network layer in OSI stack; Layer in firewall in which routing is based on IP address

MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPEG	Moving Picture Experts Group
MPTS	Multiple Program Transport Stream
MTA	Multimedia Terminal Adapter
NAT	Network Address Translation
NCS	Network Call Signalling
NE	Network Element
NG-STB-A	Next Generation STB Architecture
NIU	Network Interface Unit
OCAP	OpenCable Applications Platform
OEM	Original Equipment Manufacturer
OSS	Operations Support System
PC	Personal Computer
PHY	Physical layer
PID	Packet Identifier
PS	Portal Services
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Regional Area Network
RMS	Rights Management System
RSA	Public key cryptosystem developed by Rivest, Shamir, Adleman; also company by same name marketing public key technology
RSVP	Resource reSerVation Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SCTE	Society of Cable Telecommunications Engineers
SD	Secure Digital
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SOC	System-on-Chip
SPTS	Single Program Transport Stream
STB	Set-Top Box
SVD	Subscriber Video Device
TCP	Transmission Control Protocol

TOS	Type of Service (also DiffServ Code Point, DSCP)
TS	Transport Stream
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoD	Video-on-Demand
VoIP	Voice over IP
XML	eXtensible Markup Language

5 Conventions

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

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this Recommendation.
"SHOULD"	This word or the adjective "RECOMMENDED" 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 behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
"MAY"	This word or the adjective "OPTIONAL" 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.

6 Integrated multimedia architecture

The following are key attributes of the NG-STB-A for an *Integrated Multimedia Architecture*:

- *Expanded capacity*: Provides expanded capacity that will be non-limiting to the introduction of new services. Enables cable operator options to use spectrum more efficiently through use of: converting analog channels to digitally-compressed video services; advanced compression algorithms; more advanced modulation schemes; integrated spectrum resource management at the head-end and switched digital video.
- *All-digital transition*: Supports a transition to all-digital services while continuing economically to support legacy analog TVs and VCRs.

- *Flexible, secure conditional access (CA)*: Implements CA through internal hardware (the NG-STB-A configurable security processor, or CSP) that can be remotely configured or renewed by software downloads. Supports multiple CA options including legacy CA and new proprietary or non-proprietary CA, thus enabling integration of CPE from multiple suppliers. Provides flexibility at lower cost than physically removable CA. At the same time, cable networks can continue to support physically separable security via use of security card device.
- *Support for retail distribution*: Facilitates retail sale of subscriber video devices (SVDs) by providing capability for subscriber activation, supported by remote configuration by the operator for compatibility with any NG-STB-A cable system.
- *Secure in-home networking*: Supports open home networking technologies and standards, digital rights management (DRM) systems, and ubiquitous use of IP (Internet Protocol) for distribution of content in the home. Enables network operators to offer head-end managed multimedia home network services. Supports use of multi-room entertainment systems that employ in-home storage devices to serve content to a variety of low- and higher-end networked devices. Integrates multimedia services between formerly video-centric set-top devices and data-centric PCs.
- *Secure two-way authenticated channels*: All next generation CPE provides secure 2-way authenticated communication channels between the head-end and CPE. This increases security relative to achievable security in one-way systems. Such channels are used for renewable conditional access key management, remote management of CPE, downloadable firmware updates, private interactive application data, and reconfiguration of encryption algorithms.
- *Flexible transport options*: Supports broadcast, multicast and/or IP unicast video transport.
- *CPE equipped for future transmission and compression standards*: Allows for future increases in effective system capacity with minimal incremental investment without stranding prior CPE investments, whether such investments are made by operators or by consumers at retail.
- *Well-defined applications environment in CPE*: Includes capability for the J.200 series ITU-T Recommendations applications platform middleware to support downloadable applications, enabling rapid service creation, innovation, and new business models, with intent to run the J.200 series of ITU-T Recommendations on all SVDs subject to reasonable licensing terms. Provides the cost savings of a standard platform without limiting the ability of cable operators to innovate in the user interface and overall look-and-feel of services.
- *Rapid provisioning of new services*: Supports self-installation and rapid provisioning of new services through auto-discovery, remote management, and remote configuration features of NG-STB-A-compliant CPE.
- *Improved resource management through open head-end interfaces*: Restructuring of head-end network elements with open interfaces allows more efficient use of system resources, effectively increasing usable system capacity and flexibility, reducing cost, and expanding the number of suppliers of head-end components, while ensuring interconnection capability.

6.1 Reference architecture description

The reference architecture is defined in terms of a set of network elements that are used to meet specific needs. These network elements operate within the major network segments comprising the back-office, head-end, outside plant, and customer premises, as diagrammed in Figure 1.

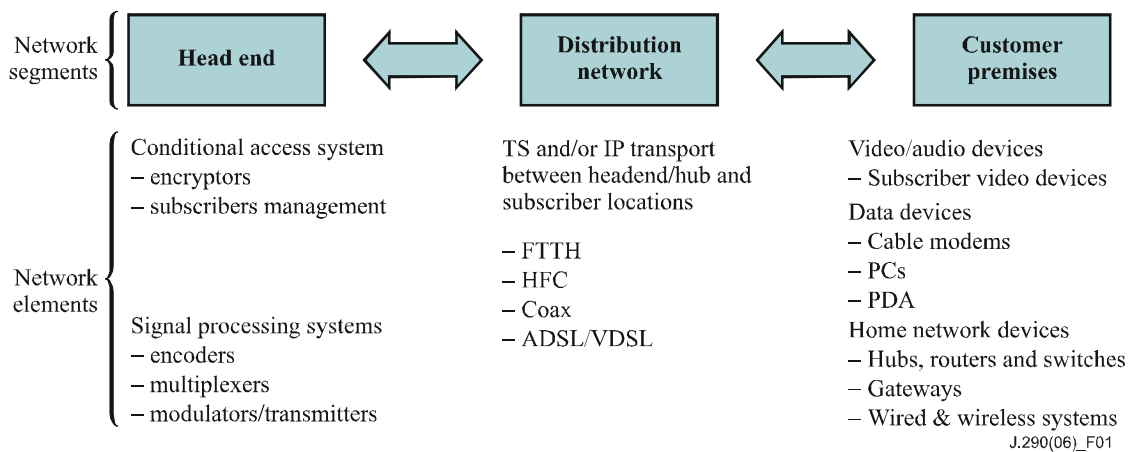


Figure 1 – Major network segments and elements

6.2 Attributes of an integrated multimedia architecture

6.2.1 Video services architecture

At a minimum, NG-STB-A-compliant CPE will have the following attributes:

- *Conditional access*: Employs reconfigurable internal CA based on a hybrid of a hardware engine for decryption (CSP) and software-defined key exchange. Supports multi-stream decryption for DVR, local advertizing insertion capabilities and other applications requiring multiple signals.
- *Video transport*: Supports two modes:
 - Non-IP mode (Baseline MPEG over QAM);
 - IP mode (MPEG encapsulated inside IP).
- *Video device applications support*: All video CPE have the minimum required resources (i.e., memory and processor power) to support [b-ITU-T J.200], [b-ITU-T J.201] and [b-ITU-T J.202].
- *Video codecs*: Support for decoding of H.262 (MPEG-2 Video) plus advanced codecs, H.264 (MPEG-4 AVC), and optionally VC-1. The client device MUST be able to switch nearly instantaneously between the currently active advanced codec and MPEG-2.
- *Audio codecs*: Supports for decoding of MPEG AAC or Dolby Digital.

6.2.2 IP multimedia architecture

- *Internet protocol*: IP selected as the basic bearer layer for all in-home network multimedia services.
- *QoS (quality of service) in IP home network*: {informative text: Plan to conform UPnP (universal plug and play standards) to enable remote management, provisioning, and service observation of UPnP devices on in-home networks.}
- *IPv6*: Support for both IPv4 and IPv6 in all IP-connected devices, with the intent eventually to transition to IPv6.

6.2.3 In-home networking

- *In-home network domains*: Defines in-home network domains as a function of level of service and of content protection.
 - GSD (guaranteed service domain): QoS managed from head-end to end device.
 - ASD (authorized service domain): Content can be transferred to receiving devices that have a certified, network operator-authenticated DRM or conditional access systems.

- OAD (output authorized domain): Content can be transferred through a rights-managed interface from the ASD to devices with non-operator-authenticated DRM.
 - BED (best effort domain): Connected devices outside of GSD, ASD or OAD.
- CPE MAY be located within any one of these domains or in multiple domains where there are overlaps.

- *USB-2 and/or Ethernet port*: Provides universal CPE connection to in-home networks. Any physical layer capable of carrying IP transparent traffic (e.g., CAT5 Ethernet) can be supported through use of an adapter between the USB port and the specific physical layer.
- *Applications sharing*: Supports applications sharing between J.200 series devices as well as non-J.200 series devices that resides in one or more of the home networking domains defined in clause 6.5.1, for example, a PC with an NG-STB-A-compatible client. Applications examples include: remote access to DVR content; multiplayer games; personal information manager (e.g., family calendar, address book, alarm clock).

6.2.4 Program insertion

- *Program insertion*: Program insertion techniques such as ITU-T Rec. J.181 (Digital Programme Insertion) supports operator needs for flexible program delivery. The ability to splice two encrypted streams together, for example to replace an encrypted content in a broadcast stream with an encrypted content previously cached on the local hard drive.

6.2.5 Network segment: Customer premises

- *Subscriber video devices (SVDs)*: SVDs are NG-STB-A-compliant video devices that include a tuner, such as set-top or set-back units or stand-alone digital TV sets (DTVs). A baseline (low end) SVD is defined with minimum required NG-STB-A functionality. Higher-end SVDs include various step-up options at the discretion of suppliers, network operators and retailers. Baseline SVD functions and examples of step-up options are listed in Table 1.

Table 1 – Baseline and extended SVD functionality

Baseline SVD functionality	Optional step-up SVD functions (Examples)
• Support for multiple transport modes • Support for decoding MPEG-2 (SD and HD) plus H.264 • In-home networking connectivity as a client • Downloadable CA • Capability for J.200-series middleware • Standard definition output • High definition video output • Digital output interfaces with copy protection • OEM provided universal remote control capable of controlling the SVD and the legacy TV • Supports J.83 QAM downstream modulation as an option • Includes general purpose USB-2 and/or Ethernet port for in-home networking connectivity and possible unspecified peripheral connection	• Copy-protected digital interfaces (e.g., HDMI, DVI) • Built-in gateway (client, server, and IP address management) function between access and in-home networks • DVR baseline functionality • VC-1 codec

- *Rights management*: CPE devices respect and protect rights of content owners over the use of their high-value content.

6.2.6 Network segment: Head-end

- *QoS & session resource management*: Defines logical structure and process flows associated with QoS (requests, grants and service assurance). Coordinates and conforms head-end QoS processes associated with all resources in head-end, outside plant and in-home network.
- *OSS/BSS interfaces*: Defines model for interfaces with back-office billing system, operations support system (OSS), and business support system (BSS).

6.3 Video services architecture

The common features of video services architecture include:

- **Security**: Configurable security processor manages conditional access (CA), copy protection, support for secure on-demand services, secure downloads, and in-home digital rights management (DRM) functions.
- **Copy protection**: Copy protection mechanisms for delivering content across protected outputs.
- **Firmware downloads**: Provides device configuration.
- **Video transport**: Support for non-IP mode (baseline MPEG over QAM) and IP mode (MPEG encapsulated inside IP).
- **Video codecs**: Support for H.262 (MPEG-2 video) and H.264 (MPEG-4 AVC) codecs, and support for SMPTE 421M (VC-1) optionally.
- **Video client software environment**: Supports J.200 series middleware in all next generation network devices that support downloadable applications, plus provide flexibility to support applications through head-end based systems.
- **Secure software download**: Support for installing and upgrading software applications, drivers, kernels and J.200 series middleware implementations.

6.3.1 Security

An SVD will include an internal next-generation configurable security processor (CSP) for managing security aspects for services. Security aspects can be categorized as follows, with some overlap:

- Device authentication and management;
- CA of services between the head-end and subscriber equipment;
- Secure download of firmware updates and downloadable applications;
- Copy protection;
- Authorized service domain security;
- DRM within devices on one or more home networks within the authorized service domain;
- A security bridge between CA and DRM is defined in ITU-T Rec. J.197.

The next generation security model includes three subsystems:

- 1) *content and key encryption/decryption*, which is hardware-based but can be remotely reconfigured;
- 2) *key management*, which is partially software-based and thus re-definable by secure conditional access system download; and
- 3) *authentication*, which is partially software-based and thus renewable by the secure CAS download.

These subsystems will support operator management of the following aspects of CA:

- Remote reconfiguration of the decryption engine to support several predefined scrambling algorithms including commonly used legacy CA algorithms as well as new CA algorithms.
- Software-defined initial download and renewability of the CA key exchange mechanism.

In the CSP reference model, content MAY be secured with either an open standard, non-proprietary CA/DRM system and/or a proprietary CA/DRM system (legacy or otherwise).

The "flexible decryption engine" in the CSP, as shown in Figure 2, is configurable to support multiple algorithms. It is flexible enough to allow configuration by remote command to be compatible with the encryption algorithms used by the CA system as well as the content protection system(s). Entitlement messages and control messages are encoded and distributed over out-of-band and in-band channels to the video CPE such that keys can be securely recovered by the CSP; this is referred to as the firmware-defined conditional access key management application.

The secure aspects of the CSP are protected by integration on a system-on-chip (SOC) that includes a configurable decryption engine and a micro-controller for key management. The SOC will include the CSP and decoder elements so that in-the-clear and compressed digital video never leaves the SOC. In-the-clear digital video will be protected between the CSP and the decoder elements of the SOC using simple hashing or fast cryptographic techniques.

The CSP will be structured to avoid incurring liability for royalties for inactive or dormant CA/DRM systems. It is expected that the intellectual property rights (IPR) related to a CA/DRM system would not be used unless and until that CA/DRM system is activated by the operator.

Examples of possible algorithm choices are shown in Figure 2. The algorithms that will be supported will ultimately be decided when specifications are developed. To support transition from legacy CA, the client device MUST possess the ability to operate in a simulcrypt or multicrypt environment. In the event that simulcrypt is enabled, the CSP will support key sharing in the CPE.

The CSP will employ technologies to support the decryption of proprietary or non-proprietary standardized secure transport streams based on such as variants of DES, 3-DES, CSA, AES and Multi2 encryption algorithms.

The CSP will be capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash and encryption keys. The next generation network will be capable of digitally signing messages used for authentication and providing integrity using a secure hash.

Each CSP in a CPE device will be identified with a completely unique ID. For private serialization, each could contain a unique identifier known as a Private Seed ID. This Seed ID is used to generate the unique key to decrypt the entitlements for that specific CPE device. The CPE device will be capable of changing the Seed ID to another unique value upon secure command from the head-end. The encryption key would then be generated using this new Seed ID as a component of the key. An asymmetric key could also be used to decrypt the category key sent in the EMM (entitlement management message).

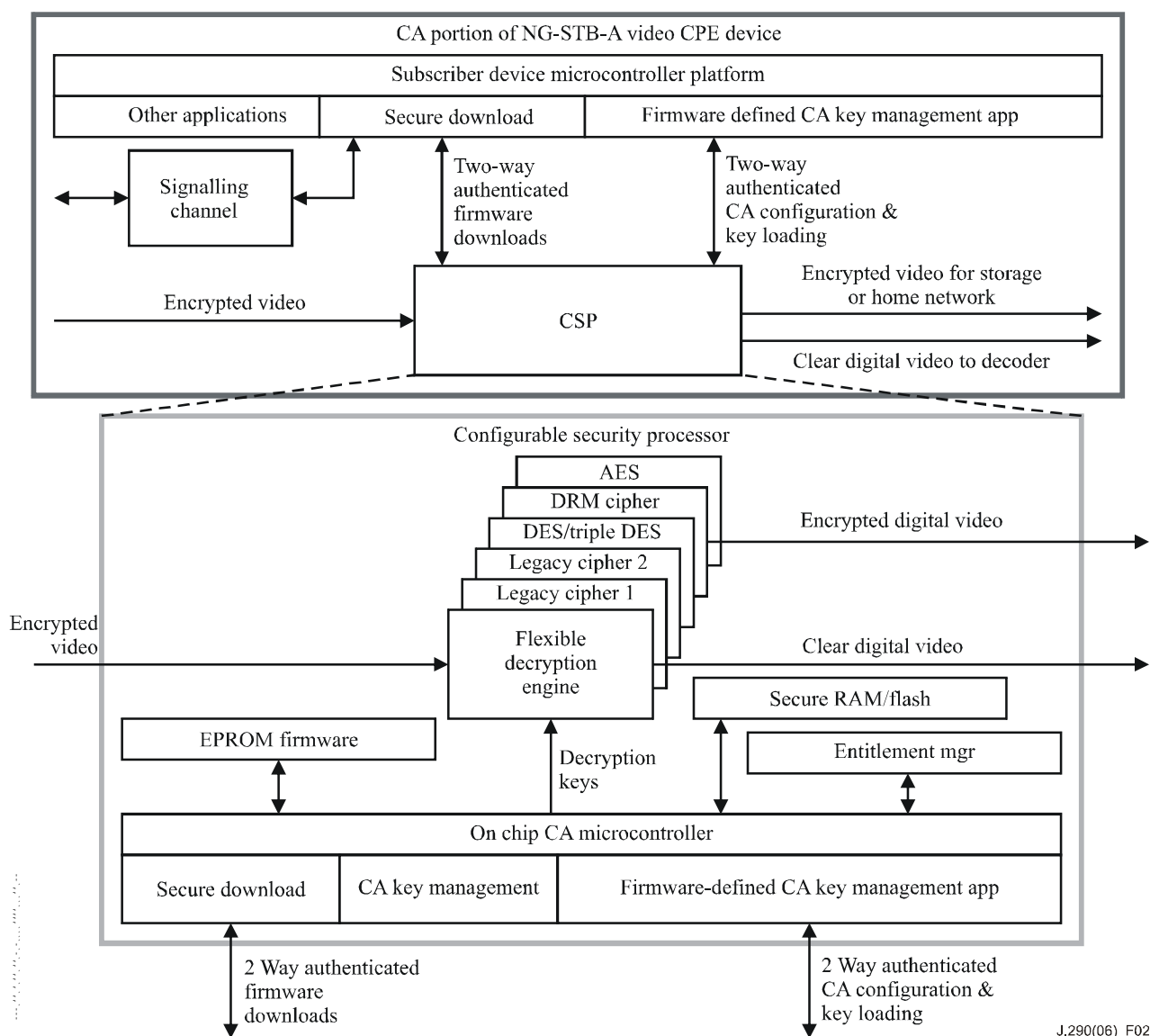


Figure 2 – Example of security block diagram

6.3.1.1 Multiple stream support

CSPs will be capable of decrypting/re-encrypting multiple content streams simultaneously. It is expected that different CSPs will be capable of processing differing numbers of streams depending on the capabilities of the associated CPE, but that all CSPs will be capable of processing some minimum number of streams simultaneously. CSPs SHOULD support the following multi-stream scenarios:

- **Watch and record:** The ability, using two tuners, to watch one encrypted stream 'live', while recording another simultaneously to a hard drive. This likely requires the CSP to remove the network CA encryption and apply a local hard drive encryption simultaneously to both streams.
- **DVR server:** DVR device with multiple tuners and a hard drive that supports other devices in the home that do not have hard drives by delivering recorded material via the home network. A DVR server can support multiple concurrent record-and-play streams, e.g., streaming content concurrently to multiple devices in the home while simultaneously recording several programs. The DVR device's CSP MAY have to support Watch and Record while also serving encrypted streams from the hard drive to remote devices in a multi-room DVR scenario.