Nagravision

China Network Systems

DIGITIZATION WITH NAGRAVISION D3 CAS (PHASE 1) SOLUTION ARCHITECTURE

0.4

NAGRAVISION S.A.
KUDELSKI GROUP

Contents

1. Introduction

This document describes the Nagravision CAS solution within the context of CNS digital platform. It consists of:

- Description of current CNS digital platform
- Description of simulcrypt architecture
- Description of Nagravision D3 CAS and features delivered to CNS

In order to deploy the Nagravision D3 CAS into the existing CNS digital platform, a thorough study has been done to understand the current configuration. This is to ensure that the deployment of the D3 CAS doesn't impact the existing services and operations.

The requirement of the initial phase of the project is described in [1].

1.1 References

Doc #	Document Title	Version	Date
[1]	CNS CAS Functional and Security Requirements	0.1	2008-03-25
[2]	Nagravision Data Importer (XML File Interface) Spec		
[3]	Nagravision Data Exporter (XML File Interface) Spec		
[4]	Nagravision SMS Gateway Interface Spec	2.7.6	
[5]	ETSI TS 101 197 DVB Simulcrypt	1.2.1	

1.2 Document History

Date	Version	Author	Description
2008-03-25	0.1	Alex Qian	Initial document
2008-04-09	0.2	Alex Qian	-Added "selection ID" requirement -Added more details on EIS<->SCS interface -Added lab BOM
2008-04-24	0.3	Alex Qian	Added SMS interface details
2008-05-29	0.4	Alex Qian	Update according to non-simulcrypt configuration

2. Current Configuration

CNS digital platform currently consists of:

- CAS: NDS
- MUX: Pegasus v3.0.12. This component is in charge of receiving and broadcasting of DVB-SI tables; It is also in charge of generating and broadcasting PSI tables
- SCS+Scrambler: Krypton v2.0.4 – Currently not simulcrypt compliant. This component is in charge of scrambling digital content, receiving and broadcasting ECM/EMM. CNS is in the process of upgrading to v3.0.9 which is a simulcrypt compliant version
- NMS: v3.0.28
- SMS: Cablesoft
- STB: ADB (ADB-ABQ-6H44) & QNS (QNS-1008)
- Middleware: NDS Core

CNS doesn't intend to keep the legacy boxes on the Nagravision platform, and new headend equipment will be purchased..

2.1 Network Topology

Following are some key points of the current CNS network:

- The **central headend** (CHE) is located in Kee Lung. This is where the digital signals are created
- There are several **remote headends** (RHE). A remote headend is the broadcast operator within a region that's not covered by the central headend. It is directly responsible for the digital signal broadcast to all the subscribers in a region
- Digital signal is propagated from CHE to these RHE, through the distribution network
- All RHE receive exactly the same signal from CHE, including:
  - Audio, Video
  - Mandatory MPEG PSI tables: PAT, PMT, CAT
  - Mandatory DVB SI tables: NIT, SDT, EIT, TDT
  - Optional DVB SI tables: BAT
  - ECM/EMM
- There is no local insertion at RHE
- There's a special case of the RHE: an external operator that receives signal from CNS and resells to their own subscribers

2.2 PSI/SI Generation and Regionalization

PSI information is currently generated by the compression system – Pegasus MUX. This includes PAT, PMT and CAT.

SI information is currently generated by NDS SI generator. This includes NIT, SDT, EIT, TDT/TOT and BAT.

Within each region, subscribers are only allowed to access services that are visible to this region. In order to enforce this restriction, CNS uses the following method:

- All RHE receive exactly the same signal from CHE

- NIT is modified manually (using the Pegasus SI editor) to match the regional frequency plan
- BAT is modified manually (using the Pegasus SI editor) to match the regional service lineup
- At initialization of a subscriber, a bouquet ID is sent to the smartcard. This bouquet ID is used for the STB to retrieve the service list. If a subscriber moves to another region, he will not be able to get any services due to the wrong bouquet ID; This could be resolved by sending the correct ID to him from the call center after he registers himself with the new location
- As a result, the modification of NIT and BAT is required everytime there's an update in these tables

The diagram below illustrates this mechanism:
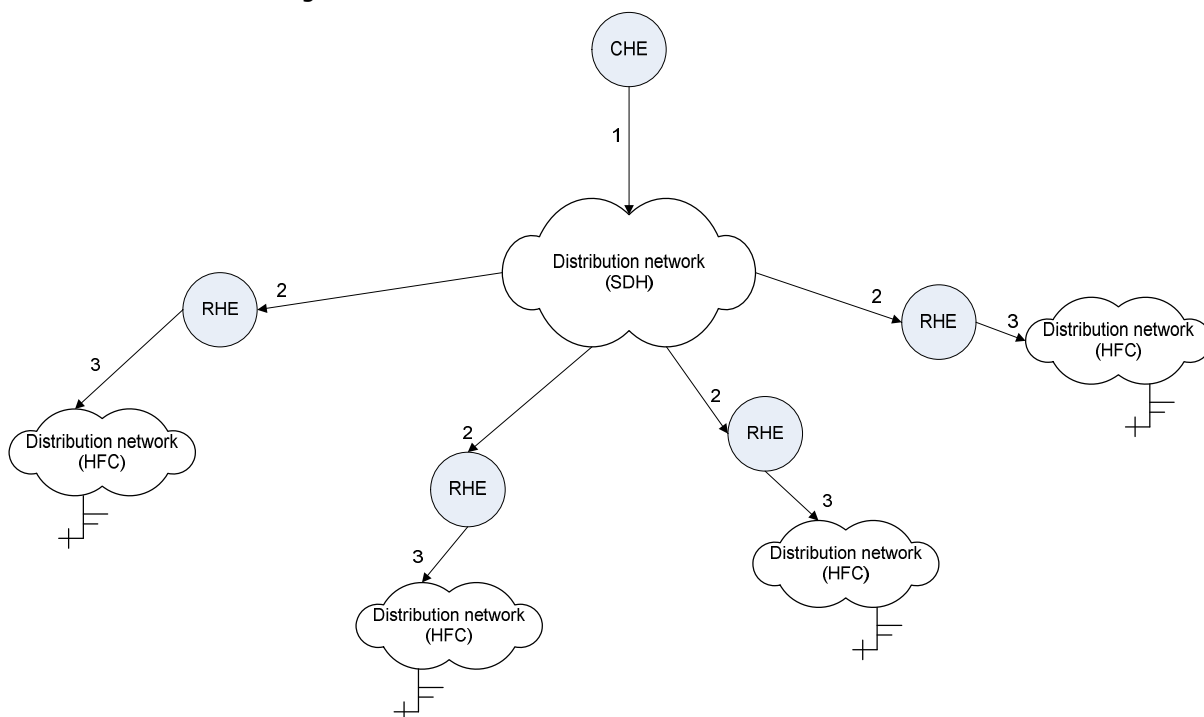
1. CHE sends its digital signal to the distribution network (SDH), including:

    • PSI: PAT, PMT, CAT

    • SI: NIT, SDT, EIT, TDT/TOT, BAT

    • Scrambled audio and video

    • ECM/EMM

2. RHE receives all of the above from the SDH network. Operator modifies NIT and BAT according to the regional configuration

3. The digital signal is rebroadcast via the regional HFC network, with the modified NIT and BAT

Besides the DVB service ID, every service is associated with a "selection ID". This selection ID is displayed by the STB as the channel number. For a given service, the selection ID could change depending on the bouquet it is in. This selection ID does not necessarily equal to the DVB service ID.

3. Nagravision D3 CAS Architecture

3.1 Overview

The diagram below shows the subsystems overview of the Nagravision CAS (highlighted in blue) and their interfaces with the rest of the CNS digital headend. The interfaces are described in more details later in this document.
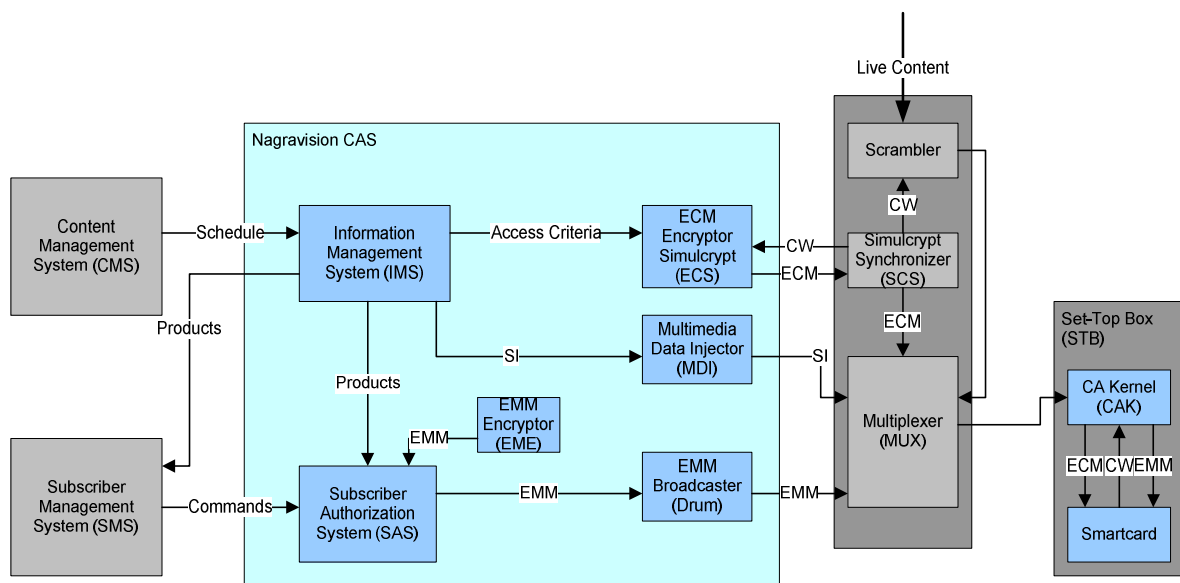
The major components of the Nagravision CAS are listed below:
- IMS
- SAS
- EME
- ECS
- MDI
- Drum

The following chapters give a summary of all these components:

3.1.1 Information Management System (IMS)

The IMS does the following:
- controlling the channel schedule information from its definition to its broadcast
- controlling the MPEG topology information from its definition to its broadcast (the topology describes the structure of the streams broadcast to the STB)
- creating pay TV products and the corresponding access criteria according to the business logic defined by the pay TV operator
- broadcasting securely (in an ECM) the access criteria and the Control Words (CW) necessary to descramble the audio/video streams (the IMS gets the CW from the multiplexer)
- generating the SI stream based on the schedule and topology information

3.1.2   Subscriber Authorization System (SAS)

The SAS does the following:
- managing and maintaining entitlements related to the broadcast content on each subscriber's smart card by sending EMMs
- offering an interface to the SMS through which the operator may grant access to pay TV products
- maintaining a precise image of each subscriber's entitlements

3.1.3   EMM Encryptor (EME)

The EMM Encryptor provides encryption and decryption services of the Entitlement Management Messages (EMM) to IMS and SAS. The encrypted EMMs are eventually broadcast by the Drum.

3.1.4   ECS/MDI/Drum

The ECM Encryptor Simulcrypt (ECS), Multimedia Data Injector (MDI) and EMM Broadcaster (Drum) are the external interfaces for ECM, DVB-SI and EMM broadcasting, respectively. The details of these interfaces are described later in this document.

3.2   Hardware Platform – Production

The table below presents the list of hardware to be delivered.

1. 2 x VTP2800: IBM Redundant P52A Servers, 1x 2-Way, 8GB, 2x146GB, FC Ctrl., Single SAN 4700 Storage (600GB); Oracle Lic. Compound Solution
2. 6 x VTP0700-ECB-AT2: EMM and ECM CAS V3 Encryptors, EMM Broadcaster.
3. 2 x VTP0720-MDI: Single Multimedia Data Injector.
4. 1 x ASI_R_SWT: DVB ASI switch for VTP0720 redundancy
5. 2 x VTP0401-FRW: NagraFire-1, 6Ports
6. 1 x TS-4: GPS Network Time Server, SYMMETRICOM S-200
7. 1 x NS5GT-005: Firewall Security VPN Router. Juniper-Netscreen 5GT-005. 100-240V 50/60Hz
8. 2 x CAB-4: 74", 42RU Rackmount 19" Cabinet with power entry
9. 2 x CAB-4-2D: Doors pair for 1 Standard Nagravision Varistar cabinet.
10. 2 x PSSW-1: Rackmount Power Supplies Auto Transfer Switch Z-Line Pulizzi T2235
11. 1 x ATP0150: Console Server; Cyclades 32 ports; cables.
12. 4 x ESW-2: Ethernet Switch. HP ProCurve 2810-24G. 20x auto-sensing 10/100/1000 ports, 1 RJ-45 serial console port, 4x dual-personality ports.
13. 2 x VTP0381-MGT: Management Workstation. HP Compaq DC7800, Windows XP, KBD and optical mouse
14. 2 x MTR-L17: 17" Active Matrix Color TFT Flat Panel HP Desktop Monitor
15. 100 x SC-TEST: Production test smart cards
16. 1 x VTP2232: IBM P52A Redundant Servers, 1x 2-Way Proc. 8GB, 2x146GB, FC Ctrl, Tape drive. Base Module.

The hardware utilization is summarized below:

- The IMS and SAS run on item 1. Also an oracle server runs on this server
- ECS, EME, and Drum run on item 2
- MDI runs on item 3. Redundancy performed by item 4
- The monitoring tool – Nagra Monitor runs on item 16
- The rest of the list includes network switch, firewall, racks, monitors, test smartcards, management station and remote support VPN.

3.3   Hardware Platform – Lab

The list below presents the list of hardware to be delivered for the lab system.

1. 1 x VTP2030: IBM Stand-alone P52A Server, 1x 2-Way Proc., 8GB, 5x146GB; Oracle.
2. 1 x VTP0700-ECB-AT2: EMM and ECM CAS V3 Encryptors, EMM Broadcaster.
3. 1 x VTP0720-MDI: Single Multimedia Data Injector.
4. 1 x VTP0401-FRW: NagraFire-1, 6Ports
5. 1 x NS5GT-005: Firewall Security VPN Router. Juniper-Netscreen 5GT-005. 100-240V 50/60Hz
6. 1 x CAB-4: 74", 42RU Rackmount 19" Cabinet with power entry
7. 1 x CAB-4-2D: Doors pair for 1 Standard Nagravision Varistar cabinet.
8. 1 x ATP0130: Console Server; Cyclades 8 ports; cables.
9. 1 x ESW-2: Ethernet Switch. HP ProCurve 2810-24G. 20x auto-sensing 10/100/1000 ports, 1 RJ-45 serial console port, 4x dual-personality ports.
10. 1 x VTP0381-MGT: Management Workstation. HP Compaq DC7800, Windows XP, KBD and optical mouse
11. 1 x MTR-L17: 17" Active Matrix Color TFT Flat Panel HP Desktop Monitor
12. 100 x SC-TEST: Smart Cards Beta Tests. 100 SC Batch.
13. 1 x VTP2000: IBM Stand-alone P52A Server, 1-Way Proc., 2GB, 2x 300GB, Tape drive

Note that the lab is:

- Non-redundant
- Only used for testing purposes
- Not used for production purposes

3.4   Production System Redundancy

This chapter describes the redundancy mechanism for every CAS component.

3.4.1 CAS Server Redundancy

Redundancy for the main servers is provided through IBM cluster solution using IBM HACMP program. HACMP (High Availability Cluster Multi-Processing) provides a computing environment that ensures that critical applications can recover quickly from hardware failures and that critical resources are available for processing. It views computer service availability not as a series of replicated physical components, but rather as a set of system-wide, shared resources that cooperate to guarantee essential services.

A cluster is made up of two independent servers (nodes) that host the application software. The nodes share resources and communicate with each other. The application data – organized in volumes – are stored on one or two shared external storages.

The diagram below shows the configuration used by CNS – a single storage HACMP cluster:
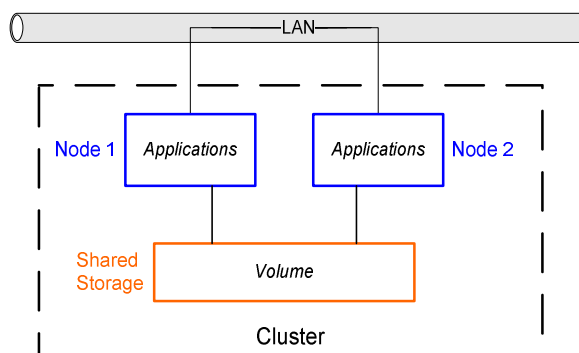
HACMP uses resource groups to manage the cluster. A resource group is a set of cluster resources containing one or several applications with, for each application:

- the volume(s) the application uses
- the IP address used by clients to communicate with the application and that is distinct from the node IP address (this IP address is called service address)

3.4.2 ECS Redundancy

The ECS servers are configured with 1+1 redundancy. This redundancy is based on the DVB SimulCrypt standard. A SimulCrypt Synchronizer (SCS) provisions the ECS with the different access groups (the SCS is provided by the MUX vendor). The diagram below shows the configuration used by CNS – 1+1 redundancy:
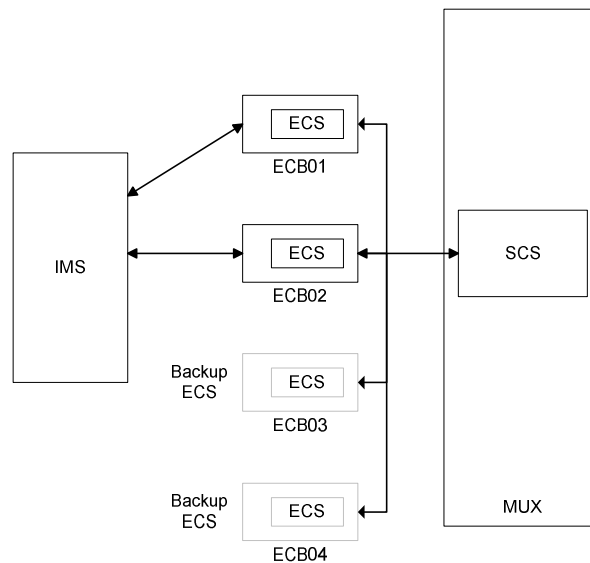
ECB01 & ECB02 run the main ECS processes; ECB03 & ECB04 are the backup ECS respectively. If one of the ECS becomes unavailable, the SCS will automatically switch to the backup ECS. Once activated, the ECS will request the different access information from the IMS. Configuration is needed on the SCS for this automatic switch.

3.4.3 MDI Redundancy

1+1 redundant Multimedia Data Injector (MDI) machines will be deployed for CNS.

Both machines of a redundant system are loaded with the same content. An ASI switch ensures the full stream availability (the ASI switch is provided by Nagravision). The diagram below shows the mechanism:
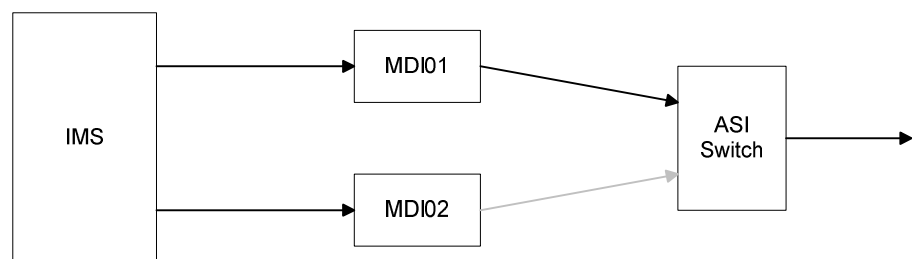
In case of a failure, the ASI switch will automatically select the available source.

3.4.4 Drum Redundancy

Two Drum servers are used for CNS, an active and a standby. The diagram below shows a possible configuration where 2 ECBs are used.
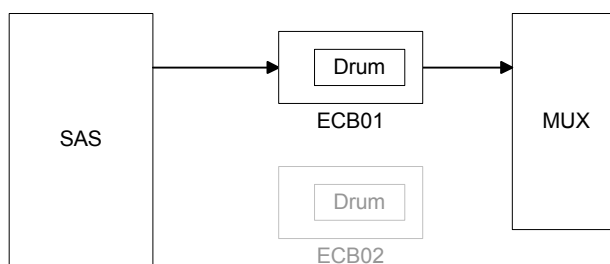
If the active Drum (running on ECB01) becomes unavailable, then the SAS needs to be manually switched to the standby Drum (running on ECB02). The standby will be reloaded using a dedicated fast reload feature.

3.4.5   EME Redundancy

EMEs are organized as a pool. The diagram below shows this concept:
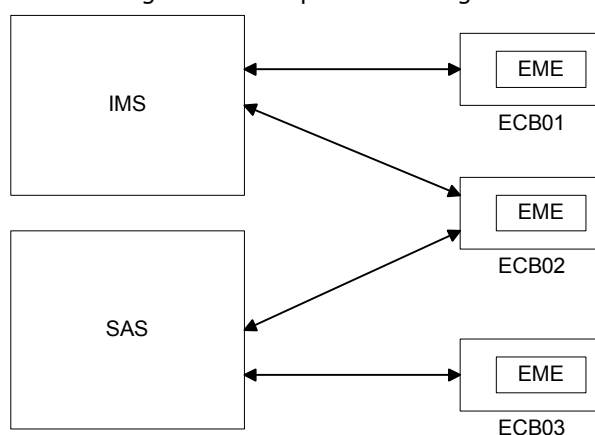
If one of these EME fails, the load will be balanced over the remaining devices.

3.5   CAS Features

The CAS features are described below according to the Nagravision CAS packaging.

The system is sized for:
- 1M active subscribers
- 200 encrypted services

Description / Axis			Remark	CAS-Packaging Production
License		CA subscribers in thousands		contract
License		Encrypted services		contract
Hardware		Max CA subscribers in thousands		1000
Hardware		Max nb of services		200
License		SI services		contract
License		PPV or IPPV services		0
License		Automated services	Video servers control	0
Pay TV Products				
	Core	Subscription		✔
	L1	OPPV		
	L2	IPPV		
	L3	Event Packages		
Pre-Paid / Post Paid				
	Core	Post-paid		
	L1	Pre-paid IPPV with return path		
	L2	Pre-paid IPPV without return path		
SI				
	Core	No SI		✔
	L1	Mandatory DVB tables		✔
	L2	DVB EIT Schedule		✔
	L3	Full DVB tables (download, etc…)		✔
	L4	Custom / Complex SI		
Schedule				
	Core	No Schedule		✔
	L1	Schedule Import		✔
	L2	Staging server (Lysis)		
	L3	iDTV		
Topology				
	Core	No edition (done at install)		✔
	L1	Topology Edition		✔
Monitoring				
	Core	Basic, terminal based		✔
	L1	Nagra Monitor		✔
Automation				
	Core	No automation		✔
	L1	Single Video Server		
	L2	Redundant Single Video Server		
	L3	Multiple Video Servers		
SMS				
	Core	SMS gateway		✔
	L1	Nagravision SMS		
Redundancy				
	Core	non redundant		✔
	L1	redundant		✔
DVR				
	Core	None		✔
	L1	Basic DVR		
	L2	Push-VOD		

Following is a list of all the business models that the CAS delivered to CNS supports.

3.5.1 Subscription

A subscriber can subscribe to one or more scrambled services by contacting the Subscriber Management System (SMS) center. Once the subscription product has been purchased, the corresponding entitlement is sent by the headend to the subscriber's smartcard so that the subscriber has access to the purchased services.

3.6 CAS Interfaces

This chapter gives a detailed description on all the interfaces between the CAS and the rest of the digital headend.
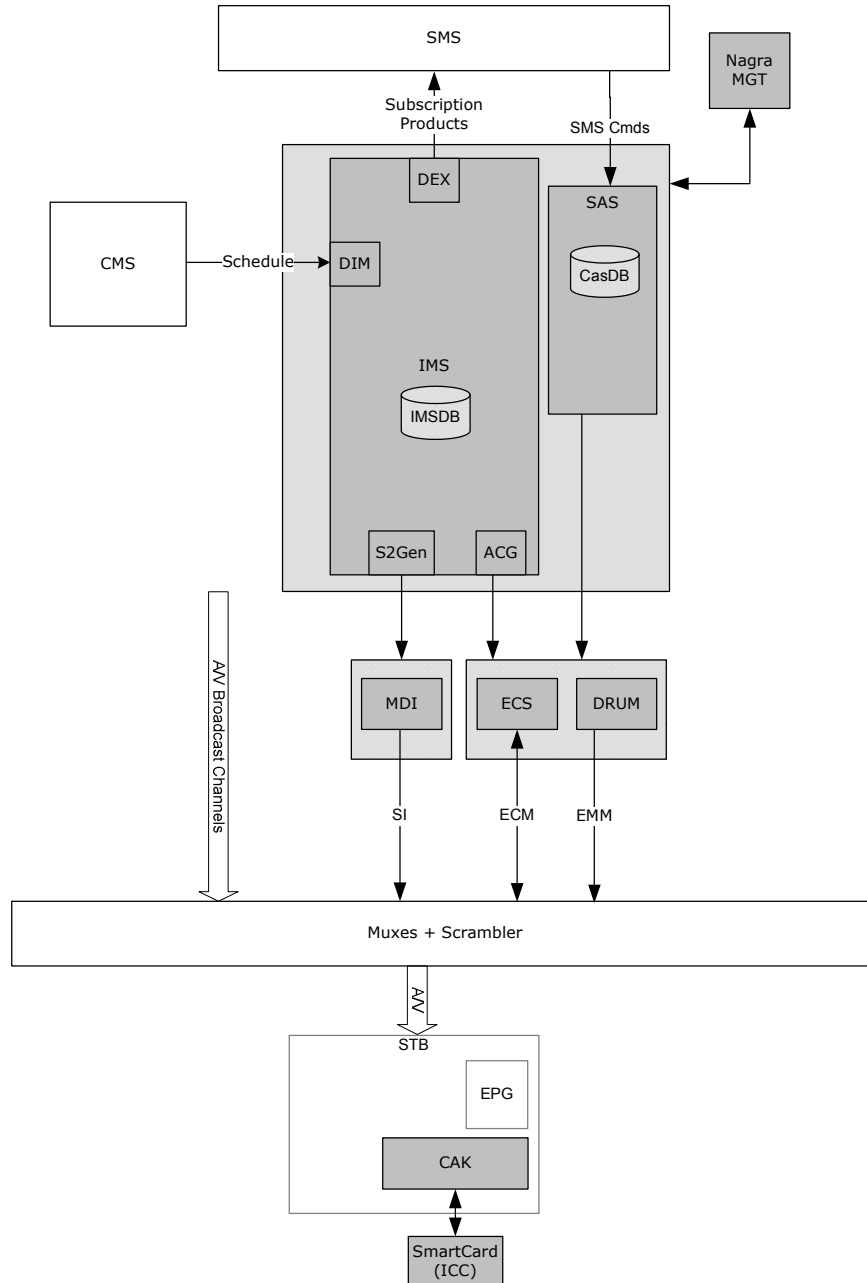
3.6.1 DIM: CMS -> IMS

Schedule Import

The Data Importer (DIM) imports data in XML format into the IMS database. It downloads the import XML files from one or several file servers. Schedule data is needed by the IMS to generate EPG (DVB EIT).

Details are given in [2]

3.6.2   DEX: IMS -> SMS

Data Export

The Data Exporter (DEX) exports data in XML format from the IMS database. It uploads the export XML files to one or several file servers. The data exported are mainly production package information (subscription products for CNS).

Details are given in [3]

3.6.3   SMS Gateway: SAS ⇔ SMS

SMS Commands

The Subscriber Authorization System (SAS) translates instructions given by the Subscriber Management System (SMS) and forwards them to the smart card.

The SAS may be connected to more than one SMS. The interface to the SMS consists of text-based messages exchanged over TCP/IP.

With the CNS configuration, the SAS can process up to 700 commands per minute.

It's important to point out that the current SMS used by CNS must be upgraded (if needed) to support simultaneous connections to both Nagravision CAS and the NDS CAS.

Details are given in [4]

3.6.4   ECMG: ECS ⇔ SCS

ECM Generation

The ECS generates, encrypts and schedules the ECM. It interfaces with the SCS according to DVB simulcrypt standard. It broadcasts the ECMs to the MUX that carousels them.

Typically the bandwidth for each ECM stream is 15kbps.

Details are given in [5]

3.6.5   EMMG: DRUM ⇔ MUX

EMM Broadcast

DRUM broadcasts and carousels the EMMs over the broadcast network. It repeats them at configurable rates to ensure a reliable and efficient delivery.

DVB Simulcrypt v1 or v2 standard can be used to connect the DRUM to the MUX

Details are given in [5]

3.6.6   SIG: MDI -> MUX

DVB-SI Generation

The Nagravision IMS will generate the DVB SI tables. The Multimedia Data Injector (MDI) broadcasts and carousels SI streams over the broadcast network.

The Asynchronous Serial Interface (ASI) protocol is used to connect the MDI to the MUX. Nagra provides one ASI output per MDI.

It's important to highlight that Nagravision is responsible for generating the SI tables only (NIT, SDT, EIT). The MUX shall generate the PSI tables (PAT, PMT, CAT). The CAT shall signal the Nagravision CAS using CAS ID 0x1805.

The table below provides the details of the CNS SI information.

Table Name	Description	Scope
NIT	Network Information Table	• Generated and broadcast by Nagravision IMS • 1 NIT Actual will be generated and broadcast for EVERY region. This PID of these NITs need to be remapped to 0x10 (DVB standard) at the remote headend • The individual NIT allows the flexibility of regionalization including different service list, frequency plan, etc. • To fulfill the "selection ID" requirement, a private descriptor will be inserted into every NIT. This descriptor will be used to associate the DVB service ID with a "channel ID" that could be different from the DVB service ID. The important thing is that the STB software must be able to retrieve and display this ID in place of the DVB service ID
SDT	Service Description Table	• Generated and broadcast by Nagravision IMS. • Carried on all transports • Bilingual with English and Traditional Chinese
EIT p/f, Actual	Event Information Table - Actual Transport Stream, Present/Following	• Generated and broadcast by Nagravision IMS • Carried on all transports • Bilingual with English and Traditional Chinese
EIT p/f, Other	Event Information Table - Other Transport Stream, Present/Following	• Generated and broadcast by Nagravision IMS • Carried on all transports • Bilingual with English and Traditional Chinese
EIT s, Actual	Event Information Table - Actual Transport Stream, scheduling	• Generated and broadcast by Nagravision IMS • Maximum EPG depth is 7 days • Carried on all transports • Bilingual with English and Traditional Chinese
EIT s, Other	Event Information Table - Other Transport Stream, scheduling	• Generated and broadcast by Nagravision IMS • Maximum EPG depth is 7 days • Carried on all transports • Bilingual with English and Traditional Chinese

| TDT/TOT | Time and Date Table / Time Offset Table | • Generated and broadcast by Nagravision IMS
• Carried on all transports. TOT will signal GMT+8 time zone |

STB Code Download

Occasionally the STB software needs to be upgraded via OTA (Over the Air) download. The software stream needs to be played out and this can be done by the Nagravision MDI.

In order to avoid overloading of the MDIs and affecting the stability of the SI generation, only one software download stream can be played at once.

3.6.7   Smartcard ⇔ STB/CAK

The CA Kernel (CAK) is the trusted representative of Nagravision CAS in the STB. It extracts EMMs and ECMs from the incoming data stream, and transmits them to the smart card. Control Words (CW) are given to the descrambler for descrambling of the stream if the smartcard contains the required entitlement.

The CNS smartcards are personalized with CAS ID 0x1805.

Glossary, terms and acronyms

ACS	*Access Control System*; Nagravision component translating SMS commands into EMMs
ASE	*Available Server Environment*; Compaq UNIX mechanism providing redundancy between a cluster of two identical machines. Used by the main CAS machines in redundant architectures
ASI	*Asynchronous Serial Interface*; protocol to interconnect DVB equipment
CA	*Conditional Access*; equipment and techniques preventing unauthorized use of data or video streams.
CAK	*Conditional Access Kernel*; Nagravision component running on the Consumer Device (or STB) and providing an interface to the security chip
CAS	*Conditional Access System*; Nagravision product, as a whole
CC	*Call Collector*; Nagravision component handling the calls from the STB to collect IPPV usage
CMS	*Content Management System*; software to manage all aspects linked to content (acquisition, scheduling, broadcasting, payments) for a Pay TV operator
DNASP	*Digital Nagravision Advanced Security Processor*; name of the Nagravision CA technology
DVB	*Digital Video Broadcasting*; Consortium of companies establishing common international standards for digital broadcasting. `<http://www.dvb.org/>`
DVB-CI	DVB Common Interface; optional digital removable security devices implementing the security and CA portions of STB in the DVB standard, functionally equivalent to the US OpenCable POD standard
ECB	Nagravision hardware device combining and ECE, EMB and EME.
ECM	*Entitlement Control Message*; CA message
ECMG	*ECM Generator*; In the context of DVB SimulCrypt, generic name given to the CA specific device or software generating ECMs.
ECO	*Engineering Change Order*; In general, procedure designed to document as precisely as possible a change in a system. Specifically, procedure by which Nagravision customers can request specific modifications to their CAS.
ECS	*ECM SimulCrypt Encryptor*; Nagravision component providing ECMs to the network; acts as a DVB SimulCrypt ECMG
EIS	*Event Information Scheduler*; In the DVB SimulCrypt system architecture, functional unit in charge of holding all the schedule information, all the configurations and CA specific information required for the complete system.
EIT	*Event Information Table*; part of the DVB SI specification
EMB	*EMM Broadcaster*; Nagravision component providing EMMs to the network; acts as a DVB SimulCrypt EMMG
EME	*EMM Encryptor*; Nagravision component encrypting EMMs before diffusion by the EMB
EMM	*Entitlement Management Message*; CA message
EMMG	*EMM Generator*; In the context of DVB SimulCrypt, generic name given to the CA specific device of software generating EMMs.
EPG	*Electronic Program Guide*; depending on the context, refers either to the STB application providing a display of the channel schedule on the subscriber TV screen, or either to the whole schedule process, from its definition, its transmission on the network to its display.
FTTH	*Fiber To The Home*; Network architecture
GUI	*Graphical User Interface*; a computer program human interface that takes advantage of the computer's graphic capabilities to make the program easier to use
IMS	*Information Management System*; Nagravision component handling the topology, schedule, and subscriber offerings (products)
IP	*Internet Protocol*
ISDN	*Integrated Services Digital Network*; set of international standards for transmitting voice, data, and video simultaneously
ISO	*International Standard Organization*
MDI	*Multimedia Data Injector*; Nagravision component streaming data or video over ATM or DVB equipment
MGT	*Management Workstations*; Nagravision supplied Windows NT computers designed to run a suite of GUIs to monitor and control the CAS

MMDS	*Multipoint Microwave Distribution System*; Wireless broadband network technology
MPEG	*Moving Picture Experts Group*; ISO working group. The term also refers to the family of digital video compression standards and file formats developed by the group
MPEG-2	MPEG second video compression scheme; coding scheme for the compression of video signals
MUX	*Multiplexer*;
Nagravision	*Nagravision S.A.*; member of the Kudelski Group of Companies, provides this document and the solutions, components or APIs it describes
NIT	*Network Information Table*; part of the DVB SI specification
NVOD	*Near Video On Demand*; principle by which the same movie or event is repeated on multiple channels at short intervals like 15 minutes
PSI	*Program Specific Information*; MPEG specifications enabling auto-tuning on the STB
SC	*Smart Card*;
SCS	*SimulCrypt Synchronizer*; In the DVB SimulCrypt architecture, logical component that acquires CW, ECMs and synchronizes their play-out for all the CA systems connected
SDT	*Service Definition Table*; part of the DVB SI specifications
SI	*System Information*; DVB or ATSC defined data format used by the STB to display information about services available on the network
SIG	*SI Generator*; In the DVB SimulCrypt architecture, component responsible for generating the SI, taking its primary data from the EIS and supplementary data from the Custom SI servers supplied by the CA providers.
SMS	*Subscriber Management System*; software program managing subscribers on the network; may be supplied by Nagravision
STB	*Set Top Box*; name of the Consumer Device in DTV networks
TCP	*Transmission Control Protocol*; main protocols in IP networks; enables two computers to establish a connection and exchange streams of data; guarantees delivery of data
TDT	*Time Definition Table*; part of the DVB SI specifications
TOT	*Time Offset Table*; part of the DVB SI specifications
VOD	*Video On Demand*; umbrella term for a wide set of technologies whose common goal is to enable individuals to select video streams from a central server for viewing on a television or computer screen
XML	*eXtensible Markup Language*; a pared-down version of SGML; allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. Nagravision uses XML for most of its APIs.