3.10.2.2 DVB-ASI

This is an asynchronous serial interface for transmitting MPEG-2 data between hardware equipment. It is described in [ASI] and is used by most manufacturers.

3.10.3 NagraVision interfaces

3.10.3.1 SMS Gateway

NagraVision defines the SMS Gateway. It describes the protocol and commands sent to the CAS. The communication protocol is a layer on top of TCP/IP. The messages contain only ASCII printable characters. For Phoenix, it will sit between the CAS Translator & Router and the CAS.

3.10.3.2 Back Channel

The public switched telephone network is used to collect data from the STB and smartcard to the Call Collector. The communication is asynchronous (V22, V22bis or better). The protocol is ISO T=1 and is entirely managed by the CA Task, in the STB, and the Call Collector. The message body is ciphered.

3.10.4 Phoenix/NagraVision interfaces

3.10.4.1 TSS-IMS-DESC

This interface is intended to provide the TSS with the NagraVision CA information or private descriptors that might be required in the APG. This information is used either for APG customization or for the impulse purchase process. The protocol is to be defined.

3.10.4.2 TSS-IMS-SCH

This interface is intended for the TSS to send to the IMS the scheduling information and PID (SCID) assignment. It is required for the ECM generation and other time based functions. The protocol is to be defined.

3.10.4.3 TSS-IMS-PRD

This interface is required for the TSS to send product definitions to the IMS. The IMS will build its own products and map the definitions into entitlement formatted for the NagraVision smartcard.

3.10.4.4 SDDS-IMS-LMC

This interface allows the SDDS to send last minute change information to the IMS. In the case of last minute change, the schedule will be modified and the next event will be affected, along with the ECM generation.

3.10.4.5 CWD-SCS-CW

This interface provides the NagraVision equipment with the Control Word to be stored in the ECM.

3.10.4.6 MDI-MUX

This interface is DVB ASI. It is used to inject ECM, EMM and IEMM into the transport stream.

3.11 Typical operation scenarios

The following sections explain some typical operations on subscriber's data. In this context, the transactions received from the CSS will be translated into the appropriate operations.

3.11.1 Subscriber management

3.11.1.1 Subscriber creation

Creating a subscriber in the NagraVision system means completing the following process:

- ?? Initialization of the subscriber's CAM;
- ?? Pairing of the CAM with the IRD;
- ?? Entering subscriber information in the system, such as the zip code.

The first two steps can occur in any order. Nevertheless, the first and the third one should be done as close as possible as it does not make sense to have initialized CAMs that are not associated with any subscriber, nor does it make sense to have an information on a subscriber who does not have a card.

3.11.1.1.1 CAM initialization

In order to be operational, a CAM must receive an initialization EMM. The CAM is initialized according to its *unique address*. A CAM can be initialized several times without altering its content.

3.11.1.1.2 CAM - IRD Pairing

To be able to operate, an IRD must be paired with a given CAM. This process will (1) enable the CAM and the IRD to operate together, and (2) will bind the CAM with the IRD so that the CAM can only be used with the IRD it has been paired with. Unless pairing data is overwritten in the CAM, the CAM is permanently paired to the IRD.

In order to pair a CAM with an IRD, the following information must be available at the SMS:

- ?? The Unique Address of the CAM
- ?? The serial number of the IRD

In almost every case, pairing of the IRD with a CAM will take place at the time of subscriber creation. However, in the case where a subscriber's CAM or IRD cannot be operated any longer, pairing may have to be performed again.

Specifically, if an IRD breaks down and is replaced, the subscriber could still use the same CAM with the new IRD, but the IRD having changed, the CAM would have to be re-paired to enable descrambling with the new IRD. In such case, only the pairing information on the CAM has to be updated, the CAM will afterwards operate just as with the previous IRD.

If a subscriber loses his/her CAM but keeps the same IRD, then a new CAM will be issued; it will have to be initialized and paired.

3.11.1.1.3 Entering subscriber information

At the time a subscriber is created in the system, the following information must be available to the SMS:

- ?? The UA (Unique address = ID) of his/her CAM. This information is printed on the CAM or displayed on the TV screen (fingerprinting).
- ?? The ZIP code
- ?? Phone number(s)
- ?? Values for initial credit and threshold
- ?? The various phone numbers of the call collectors the CAM will report to
- ?? The date of the first callback
- ?? The period between two callbacks

The subscriber creation process includes the following operations (in sequence):

- ?? Create CAM on Call Collector, to create the CAM in the database of the Call Collector in order for callbacks to be processed.
- ?? Set Zip Code, the CAM must know its location zip code since time information and possibly blackout information are based on the subscriber's location.
- ?? Define Credit Limit, to set the credit limit.
- ?? Set Call Collector Phone Numbers
- ?? Enable Automatic Call Back (optional). This command includes call time calculation by the Call Collector.

3.11.1.2 Subscriber suspension

Entitlements stored on a CAM can be temporarily suspended in three different ways:

- ?? Suspend one entitlement only.
- ?? Suspend Impulse Purchase.
  This command is used to suspend the possibility to perform impulse purchases of IPPV programs. The subscriber may still call the SMS to order products.
- ?? Suspend CAM.
  This command temporarily disables all entitlements and the possibility to perform impulsive purchase IPPV programs.

Entitlements or CAM suspension do not prevent callbacks from occurring.

3.11.1.3 Subscriber removal

To remove a subscriber from the system, the following operations must be performed:

- ?? Remove all entitlements from the CAM. It will not remove the IPPV watched and not call collected
- ?? Force immediate callback
- ?? Remove impulse purchase capability and purchase balance

If the CAM is removed from the IRD before the last callback occurred, all IPPV purchased may still be retrieved when the CAM is inserted into an IRD. The IRD can then be reused.

3.11.2 Product management

All products are created either manually, with the IMS editor, or with the SMS Gateway commands 300 series, or with the interface between the TSS and the IMS.

3.11.2.1 PPV product creation

In order to create a PPV product, the following steps are performed:

?? Assign a PPV number to the event. This number is selected depending on the kind of package. For example, if it is a unique event, then the number will be unique during a time frame of 3 days. If this event is part of another package, then the PPV number will be selected in the range granted by the package.

?? Create a PPV product granting access to the number selected. For complex packages, the range of numbers can be arbitrarily created.

Subscribers need to call the customer center to purchase the product.

3.11.2.2 IPPV product creation

This type of product is created the same way as PPV products. The only difference is that an IEMM will also be created, in order to allow the subscriber to purchase the product impulsively, using the credit on the smartcard.

3.11.2.3 Blackout assignment

Blackout characteristics can be assigned during the product creation or after. When blackout restrictions are assigned to the products, then private descriptors are made available by the IMS. They can be inserted in the APG, in order to prevent the purchase of a product by a subscriber living in an area subject to blackout.

3.11.2.4 Product modification

Products can be modified at any time. The product modification is not reported to the subscribers that may already have purchased the product. In this case, if the product has already been sold, there are two possibilities:

1/ Create a new product instead of modifying the existing one and send the new product definition to the subscribers that have already purchased the product. This can be done by using SMS Gateway commands.

2/ Send entitlement modification commands to the smartcards of the subscribers that have already purchased the product, or to all smartcards that already contain the product. This cannot be done through the SMS gateway, but by the IMS, under certain restrictions.

3.11.3 Channel lineup change

Channel-lineup modifications require the IMS to know the new topology. Topology includes PID (SCID) and transponder allocation for all channels. Topology modification does usually not affect the access conditions, or the NagraVision private descriptors content. Topology is provided to the IMS by the interface TSS-IMS-SCH.

3.11.4 Last minute change

Last minute change is provided to the IMS through the interface SDQS-IMS-LMC. Its effect is to change the scheduling of the next events in the schedule. A signal will also be sent to the ECM generator and the ECM encryptors in order to take the change into account. A last minute change should occur more than two minutes before the transition to the next event.

3.11.5 Stolen smartcard management

Stolen cards or lost cards are not useable anymore by the CAS. A special SMS Gateway command is used, telling the CAS that the card has to be killed and preventing it to send EMM messages addressed to this card. Only globally addresses EMM can be sent to this card.

4. Head-end architecture

This chapter gives a detailed description of the head-end architecture and features.

4.1 Overview

This section presents the various modules in a very high level view. The following picture illustrates the various software modules of the NagraVision CAS and their interactions. Modules are shown within the machine they run on; please refer to the previous section for hardware information. Obvious inter-process communications are not shown for picture legibility.

Phoenix specific devices are shown for clarity only. They are described in the previous chapters and will not be detailed here.

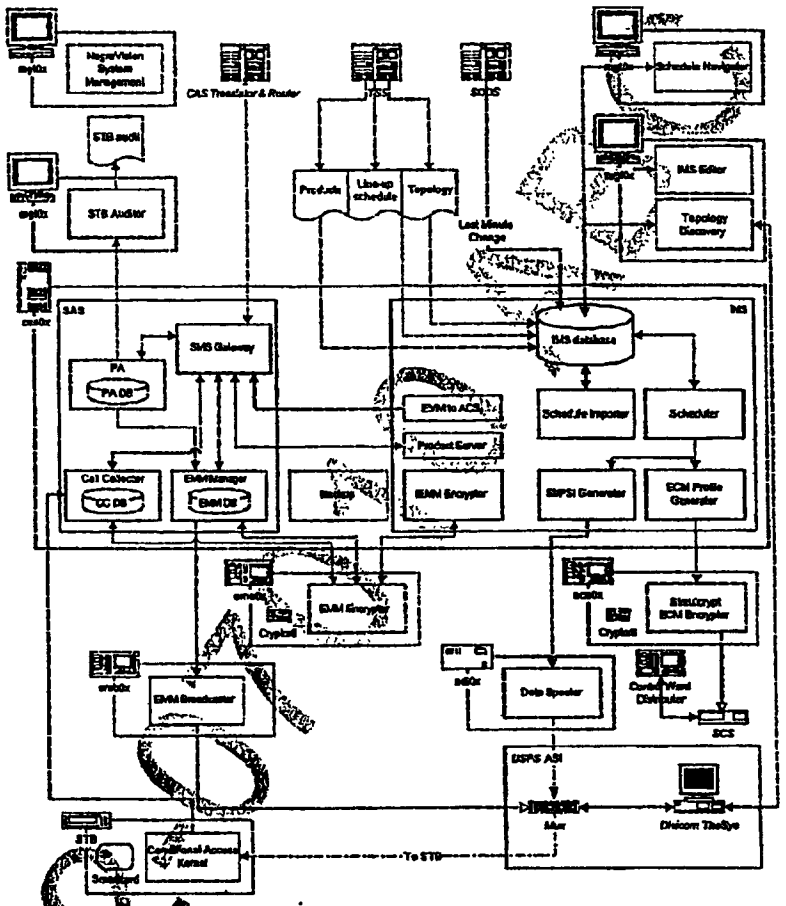

Figure 4.1

4.1.1 Information Management System (IMS)

The Information management System (IMS) is a sub-system managing logical links between different parts of the system: network topology, products and event profiles. The main task of the IMS is to control and follow the evolution of pay-events from their definition until their broadcast.

It is composed of many modules:

?? IMS Database contains the network topology, services and event definitions and products
?? Schedule Importer (SCI) allows importation of event data from an ASCII-delimited file.
?? Scheduler provides starting signals to different tasks when a new event starts.
?? ECM Profile Generator: generates the ECM profiles for the ECM Encryptor when a new event starts.
?? ECM Encryptor encrypts ECM and broadcasts them to the muxes.
?? IEMM Encryptor: creates all information needed by the system for impulse purchase of PPV.
?? Product Server: provides products and rights definitions to the SMS Gateway.
?? EPG Generator generates all DVB SI tables for the IRD.
?? Data Spooler continuously broadcasts SI information to the IRDs.
?? Product Gateway provides an ASCII-delimited file interface to the ICMS for IPPV product creation.
?? EMM to ACS allows the IMS modules to send EMMs

Additional modules are provided to manage or monitor the IMS data:

?? IMS Editor allows the creation and modification of all data handled in the IMS Database
?? Topology Discovery manages the network topology
?? Schedule Navigator displays all channels and events broadcast

4.1.2 Subscriber Authorization System (SAS)

SAS is responsible for managing EMMs that have to be sent down to the STBs. It is composed of the following modules:

?? SMS Gateway serves as the CAS control interface for the ICMS
?? EMM Manager (EMGR) creates, manages and stores EMMs
?? EMM Encryptor (EME) encrypts the EMMs
?? EMM Broadcaster (EMB) broadcasts EMMs to the multiplexing equipment
?? Positive Addressing (PA) refreshes entitlements on a regular basis
?? Call Collector (CC) collects IPPV usage information and holds subscriber information in its database

Additional modules are provided to manage or monitor the SAS data:

?? STB Auditor allows reporting of STB product provisioning to an ASCII-delimited file.

4.1.3 Other modules

The following modules are part of the CAS, but do not belong to the IMS or SAS:

?? Conditional Access Kernel is the interface between the smartcard and the STB
?? Backup provides daily backup and cleaning of databases and file-system
?? NagraVision System Management (NSM) monitors and control the CAS
?? SNMP Gateway provides a SNMP interface for remote monitoring

4.2 Detailed features

4.2.1 Backup

4.2.1.1 Description

This module provides a daily backup and housekeeping service for the entire CAS. Every day, Backup:

?? Creates a dump file of the IMS Database in the backup directory
?? Creates a dump file of the EMM Database in the backup directory
?? Creates a dump file of the CC Database in the backup directory
?? Creates a dump file of the PA Database in the backup directory
?? Stores the backup directory on tape. In addition to the database dumps, the backup directory is also the default location for all files processed or generated by the CAS, such as Schedule Importer files
?? Erases old Schedule Importer file
?? Erases old events in the IMS Database
?? Erases old products in the IMS Database and PA database
?? Erases old SMS Gateway feedback commands in the IMS Database

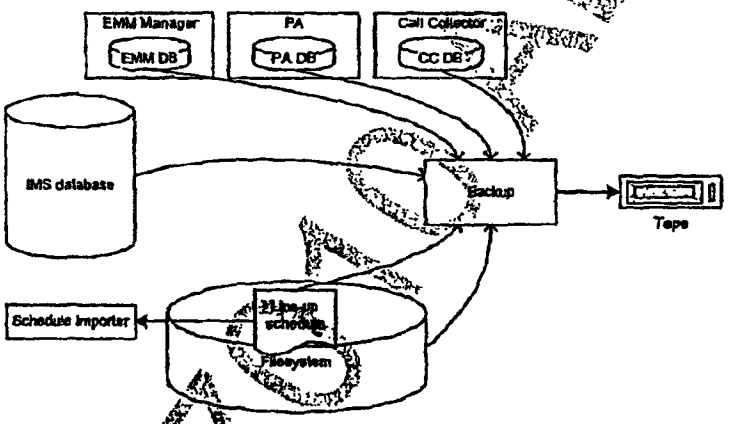

Figure 4.2

Generally, 7 days of history are kept for all items, except for the Call Collector database where 2 months are kept.

All other components not mentioned here, such as EMM Broadcaster or Topology Discovery, store only static data on their local machine and therefore do not need daily backup service. Product Gateway files are under the responsibility of the operator for backup and housekeeping, as described in [SMS_IPPV].

The only manual operation needed is to insert a tape into the drive every day. The tape is ejected at the end of the operation. Backup is configured to run at a specific time of the day.

To guaranty the integrity of the backups, the EMGR database needs to be put offline during its dump procedure (commands 0-99 are packed with nack-status to POSTPONED).

4.2.1.2 Interfaces

By default, this module exports the *tar* file to the tape drive, but this could be redirected to another location if required.

4.2.1.3 Performance

Backup needs about one hour per day to perform all its tasks. This is generally scheduled to happen during the night. The dump of the EMM Database lasts a maximum of 10 minutes.

4.2.1.4 Scalability

Some advanced backup database strategies are available if more frequent backups are needed.

4.2.1.5 Redundancy and Availability

The watchdog monitors this module. Backup only operates at its scheduled time, and does nothing if restarted many times a day.

4.2.1.6 Manageability

All aspects of this module are configured through text-based configuration files and scripts.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.2.1.7 Failover Recovery

If one of its steps fails, Backup appropriately informs the operator through console messages and logs, then stops all operations. For example, if the tape write operation is not possible (no tape in the drive, for example). Backup does not erase anything. In these cases, the backup procedure must be started manually if a backup is desired for this particular day.

4.2.1.8 Security

This section does not apply to this module.

4.2.1.9 PHOENIX Customizations

This module will be tailored to PHOENIX environment at installation time.

4.2.2 NagraVision System Management (NSM)

4.2.2.1 Description

The NagraVision System Management (NSM) is a tool designed to manage the NagraVision Conditional Access System (CAS). This tool can assist a system manager to:

- ?? Configure each component of the CAS (Configuration Management)
- ?? More efficiently detect, isolate, and recover the cause of a malfunction (Fault Management)
- ?? Tune precisely the performance of the system (Performance Management)
- ?? Define the security level required by some functions of the system (Security Management)
- ?? Monitor and control the system to manage through a console.

For a detailed description of NSM, see [NSM].

4.2.2.2 Interfaces

The SNMP Gateway module provides an external interface to this module by allowing the most important alarms and messages to be available on SNMP. See 4.4.22.

4.2.2.3 Performance

See [NSM].

4.2.2.4 Scalability

See [NSM].

4.2.2.5 Redundancy and Availability

The NSM module is an interactive application. Its availability is not critical to the CAS.

4.2.2.6 Manageability

See [NSM].

4.2.2.7 Failover Recovery

See [NSM].

4.2.2.8 Security

See [NSM].

4.2.2.9 PHOENIX Customizations

New modules developed following NagraVision software standards will be monitored and managed by NSM.

4.3 Component description

4.3.1 IMS Database

4.3.1.1 Description

The IMS Database is an Oracle 7.3.2 database that stores the following information:

- The network topology (elementary streams, transponders), including Access Control Groups
- Service definitions, including conditional access information
- Event schedules, descriptions, blackout regions, etc.
- Product and entitlement definitions
- Blackout type and subtype definitions

4.3.1.2 Interfaces

This section does not apply to this module.

4.3.1.3 Performance

The database is optimized at the factory to deliver the best possible performance on the specific hardware used.

The maximum duration of the data history in the IMS Database is two weeks. Having more history than this affects IMS performance. The Backup module is generally configured to keep only 7 days of history data inside the IMS Database.

4.3.1.4 Scalability

Oracle configuration and Oracle tools provide scalability.

4.3.1.5 Redundancy and Availability

DECsafe ASE manages the underlying hardware and the database processes.

4.3.1.6 Manageability

The IMS Database is configured using command line tools provided by Oracle and text configuration files. The Oracle database maintains a log file.

Oracle MIBs are standard and provided by Oracle.

4.3.1.7 Failover Recovery

A database crash is often recovered just by restarting the database. If this is not possible, the IMS Database may be rebuilt from its last backup.

Modules connecting to the database are designed to handle IMS Database failures; they either:

- Terminate immediately (in which case the watchdog restarts them after a predefined interval. They reconnect to the database and continue processing as soon as the database is available.
- Stay up in a disconnected idle state and try periodically to reconnect

Interactive applications running on the CAS workstations have to reconnect manually to the database.

4.3.1.8 Security

Security is handled by standard Oracle procedures, that is, username and password. Interactive applications, such as Topology Discovery, explicitly ask for the Oracle authentication information. Other modules, such as Scheduler, use a constant account to log on to the database.

4.3.1.9 Phoenix Customizations

To be defined during detailed analysis phase.

4.3.2 Schedule and Topology Importer

4.3.2.1 Description

The Schedule and Topology Importer is an internal IMS process responsible for importing schedule data files and Transport configuration information into the IMS Database. This information is used later to schedule ECM profiles and provide PID allocation to the IMS.

Schedule data contain the schedule information for a number of services and events over a given period of time.

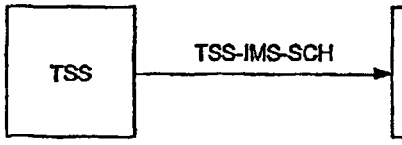

Figure 4.3

4.3.2.2 Interfaces

There is a document [IMS_IBS] already describing an existing protocol. It will be modified for Phoenix specific needs.

4.3.2.3 Performance

Schedule Importer is able to process at least 2 events per second.

4.3.2.4 Scalability

The limiting factor in Schedule Importer performance is the IMS Database. Hence, this process is not easily scalable.

4.3.2.5 Redundancy and Availability

The watchdog continuously monitors this process and restarts it if necessary. DECsafe ASE manages the underlying hardware.

4.3.2.6 Manageability

Schedule Importer is configured using a text configuration file. The IMS provides a command line tool to monitor this process, and to restart it if necessary. Errors are sent to a log file and to an error log stored along the file in error on the RAS.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.3.2.7 Failover Recovery

This section does not apply to this module.

4.3.2.8 Security

This section does not apply to this module.

4.3.2.9 Phoenix Customizations

This module is adapted to the Phoenix Schedule File format defined above.

4.3.3 Scheduler

4.3.3.1 Description

The IMS Scheduler manages all IMS operations requiring synchronization between the EPG generation and ECM generation.

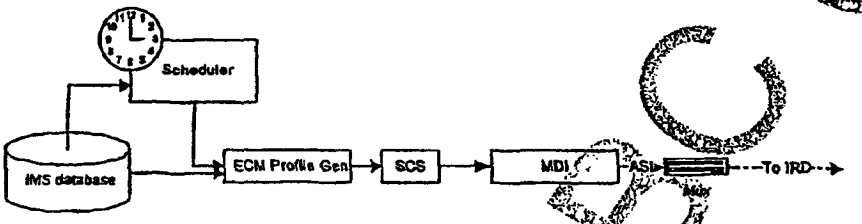

Figure 4.4

The scheduler reads in its memory the list of events that will occurs in the next 4 hours. It also contains a clock that tells the current date and time. With this information, Scheduler knows when a new event shall start, and sends TCP/IP messages on the network to interested modules, such as ECM Profile Generator.

The messages contain an event identifier (event ID) and are the following:

?? Event will start. It is sent 2 minutes before an event starts.

?? Event is starting. It is sent at the precise time when an events starts.

?? Next event. When an event starts, it contains the ID of the next event.

?? Date and time. It regularly sends the current date and time.

Depending on the functions of the interested modules, they may only need a subset of these messages. For example, the EPG Generator needs the current date and time and the ECM Profile Generator needs to know when a new event will start.

4.3.3.2 Interfaces

This section does not apply to this module.

4.3.3.3 Performance

This section does not apply to this module.

4.3.3.4 Scalability

This section does not apply to this module.

4.3.3.5 Redundancy and Availability

The watchdog continuously monitors this module and restarts it if necessary. DECsafe ASE manages the underlying hardware.

4.3.3.6 Manageability

Scheduled tasks are configured through a text based configuration file.

The IMS provides a command line tool to monitor this process, and to restart it if necessary.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.3.3.7 Failover Recovery

This section does not apply to this module.

4.3.3.8 Security

This section does not apply to this module.

4.3.3.9 Phoenix Customizations

There is no customization required.

4.3.4 ECM Profile Generator

4.3.4.1 Description

The ECM Profile Generator generates an ECM profile each time a new event starts within a given service. The scheduler informs the ECM Profile Generator of the event 2 minutes before it starts. The profile specifies the start and stop times for the event and the access profile for the event. The profile is updated for a service with each event change, regardless of whether the access profile for that service changes on a per-event basis.

The access profile describes whether or not an event is protected. If the event is protected the profile describes the rights required to view the event and optionally, the regional "black-out" or "spotlight" areas that restrict the viewing of an event in specified regions or allow events to be viewed in specified areas.

These viewing regions are defined by inserting the restricted or allowed blackout definitions into the ECM. A subscriber is then only able to gain access to a regionally controlled service if the blackout definition specified in the ECM does not conflict with the blackout configuration stored on the subscriber's smartcard.

The ECM Profile Generator can support free preview periods at the beginning of protected events. This preview period can be defined per service or overridden at an event level.

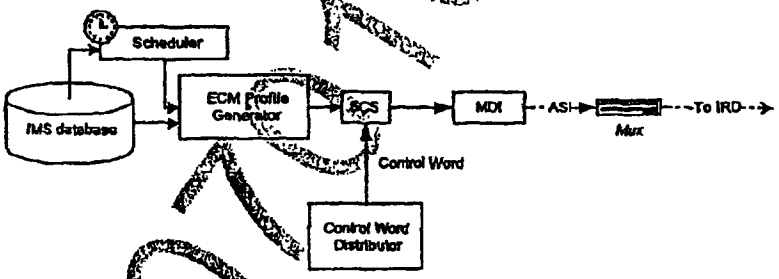

Figure 4.5

The ECM Profile Generator is responsible for providing the ECM Encryptor with the new ECM profile 2 minutes before the new event starts. It sends a message containing the ECMId and event profile. The SCS receives the message and acknowledges it. If the ECM Profile Generator receives no acknowledge after a timeout period, the message is sent again and again until a new event starts or acknowledge is received.

4.3.4.2 Interfaces

The protocol is internal to NagraVision.

4.3.4.3 Performance

This section does not apply to this module.

4.3.4.4 Scalability

This section does not apply to this module.

4.3.4.5 Redundancy and Availability

The watchdog continuously monitors this module and restarts it if necessary. DECsafe ASE manages the underlying hardware.

4.3.4.6 Manageability

The IMS provides a command line tool to monitor this process, and to restart it if necessary.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.3.4.7 Failover Recovery

This section does not apply to this module.

4.3.4.8 Security

This section does not apply to this module.

4.3.4.9 Phoenix Customizations

This section does not apply to this module.

4.4 ECM Encryptor (ECE)

4.4.1 Description

The ECM Encryptor (ECE) is responsible for creating and encrypting ECMs. The step-by-step process is the following:

- An ECM profile is supplied to the SCS by the ECM Profile Generator
- A control word supplied by the control word distributor is supplied to the SCS
- Control word and ECM profile are provided to the ECE, for ECM building and encryption
- Encrypted ECM is returned to the SCS
- ECM is sent to the MDI for broadcasting

The ECE is able to make the link between the two items using an identifier, the ECM_id. This identifier is created when the topology is imported from the TSS.

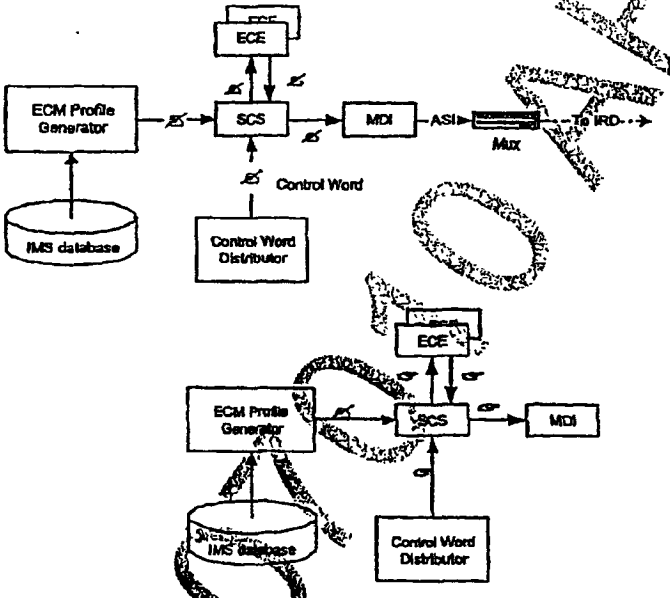

Figure 4.6

The ECM is encrypted using a mother smartcard.

4.4.2 Interfaces

The interfaces between the ECM profile generator, the SCS and the ECE are DVB Simulcrypt compliant [DVB_SIMUL]. This compliance is not required for the scope of this project, but it provides flexibility for future improvements.

4.4.3 Performance

One ECE is required for every 50 services with a 5 seconds crypto-period.

The ECMs are broadcast by the MDI.

4.4.4 Scalability

ECE can be added linearly when more services are on-air.

4.4.5 Redundancy and Availability

Each ECE is monitored by its own watchdog.

Redundancy is handled by the SCS. The ECE are completely interchangeable. It is up to the SCS to handle any error with a particular ECE, and to ask another one for the same information.

4.4.6 Manageability

The IMS provides a command line tool to monitor the ECE, and to restart it if necessary.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.4.7 Failover Recovery

A failed ECE is operational as soon as it comes back online. The SCS needs not to be manually informed about it, as the failed ECE is considered as a redundant by the SCS (and therefore will be tried if the one in use was to fail).

4.4.8 Security

Each ECE module is secured by a mother smartcard. With this concept, non-authorized access to sensitive information is avoided.

4.4.9 Phoenix Customizations

There is not modification required to the ECE.

4.4.10 Simulcrypt synchronizer (SCS)

4.4.10.1 Description

The simulcrypt synchronizer (SCS) is responsible for distributing control words to the various ECE and managing the ECE redundancy.

The step-by-step process is the following:

- An ECM profile is supplied to the SCS by the ECM Profile Generator
- A control word supplied by the control word distributor is supplied to the SCS
- Control word and ECM profile are provided to the ECE, for ECM building and encryption
- Encrypted ECM is returned to the SCS
- ECM is sent to the MDI for broadcasting

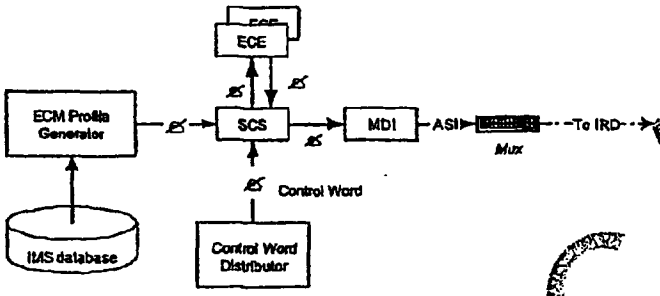

Figure 4.7

4.4.10.2 Interfaces

The interfaces are DVB Simulcrypt compliant [DVB_SIMUL]. This compliance is not required for the scope of this project, but it provides flexibility for future improvements.

4.4.10.3 Performance

SCS upper limit has not been measured over 500 services.

4.4.10.4 Scalability

Additional SCS can be installed, but the control word distributor must support the multi-SCS configuration.

4.4.10.5 Redundancy and Availability

The SCS has its own watchdog and restarts it if necessary.

The control word distributor must handle redundancy.

4.4.10.6 Manageability

The SNMP Gateway allows an external system to read this module state and other basic info rmation. See 4.4.22.

4.4.10.7 Failover Recovery

A failed SCS is operational as soon as it comes back online. The control word distributor will automatically be notified.

4.4.10.8 Security

This section does not apply to this module.

4.4.10.9 Phoenix Customizations

This module needs to be integrated with the control word distributor.

4.4.11 IEMM Encryptor

4.4.11.1 Description

IEMM Encryptor is responsible of creating the IEMMs needed to support impulsive purchase of events. The IEMMs are broadcast like EMM, on a separate PID. Upon the purchase of an event at the STB, it extracts the IEMM from the IEMM stream and passes it to the smartcard. Provided the smartcard still has enough credit, the entitlement is added to the smartcard and the event may be descrambled.

IEMM Encryptor is driven by the product creations provided through the interface TSS-IMS-PRD. Whenever a new impulsively purchasable product lacking an IEMM is found, IEMM Encryptor creates the IEMM, hands it to the EME for encryption, then sends the resulting encrypted IEMM to the EMM manager (SAS). The IEMM broadcaster will later broadcast the IEMM.

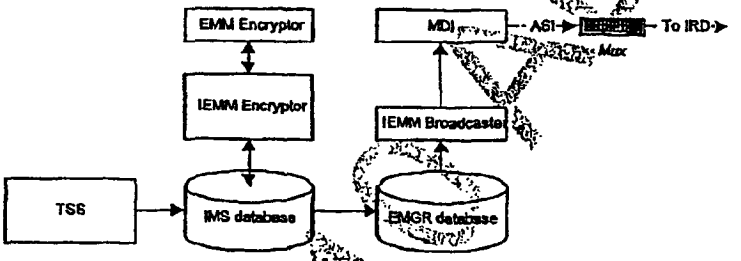

Figure 4.8

4.4.11.2 Interfaces

This section does not apply to this module.

4.4.11.3 Performance

The performance of IEMM Encryptor is directly bound to the performance of the EMM Encryptor.

4.4.11.4 Scalability

EMM encryptors can be added.

4.4.11.5 Redundancy and Availability

The watchdog monitors this module, and DECsafe ASE manages the underlying hardware and database.

4.4.11.6 Manageability

This module manages a log file for errors and is configured using a text configuration file. The IMS provides a command line tool to monitor this module, and to restart it if necessary.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.4.11.7 Failover Recovery

This section does not apply to this module.

4.4.11.8 Security

This section does not apply to this module.

4.4.11.9 Phoenix Customizations

This section does not apply to this module.

4.4.12 Product Server

4.4.12.1 Description

Product Server provides the SMS Gateway with products and rights definitions. When the SMS Gateway receives a subscription-related command, it gets from Product Server all data needed to build the EMM that have to be sent to the subscribers when they order or cancel a product.

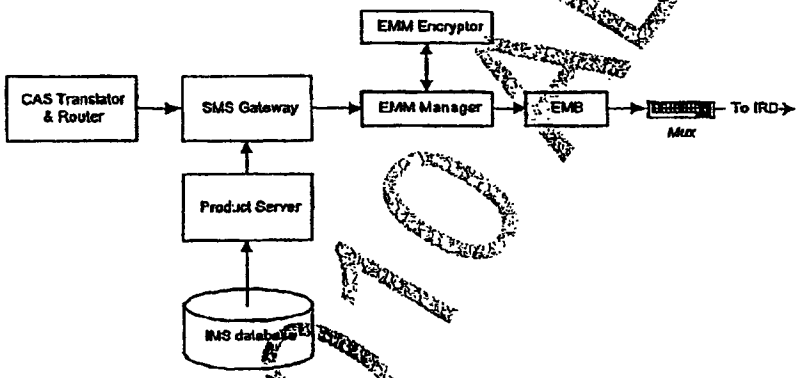

Figure 4.9

4.4.12.2 Interfaces

This section does not apply to this module.

4.4.12.3 Performance

Product Server is able to provide at least 10'000 products definitions to the SMS Gateway.

4.4.12.4 Scalability

Product Server is bound to the scalability of SMS Gateway.

4.4.12.5 Redundancy and Availability

The watchdog monitors Product Server, and DECsafe ASE manages the underlying hardware and database.

4.4.12.6 Manageability

Product Server manages a log file for errors and is configured using a text configuration file.

The IMS provides a command line tool to monitor this process, and to restart it if necessary.

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.4.12.7 Failover Recovery

Product Server has been designed to withstand communication failures with the SMS Gateway. In case of bad connections, it simply stays idle and tries to reconnect at regular intervals.

4.4.12.8 Security

This section does not apply to this module.

4.4.12.9 Phoenix Customizations

This section does not apply to this module.

4.4.13 Multimedia Data Injector (MDI)

4.4.13.1 Description

The MDI is a general-purpose data injector. It provides DVB ASI input/output and Ethernet interfaces.

It is used to broadcast EMM, IEMM and ECM.

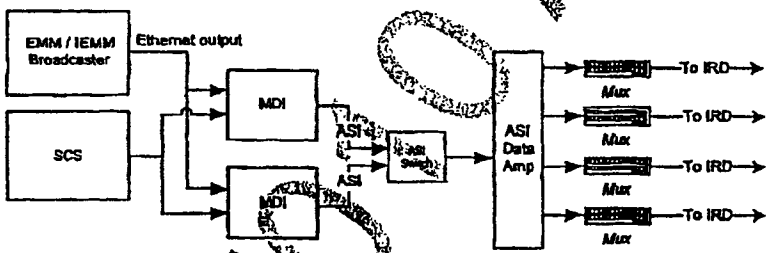

Figure 4.10

4.4.13.2 Interfaces

The MDI inputs are DVB ASI and Ethernet.

The MDI output is a DVB ASI interface. See [ASI] for information on this protocol.

4.4.13.3 Performance

Performance is limited by the hardware ASI interface at 25 Mbits/s.

4.4.13.4 Scalability

One MDI is required for every 4 transponders.

4.4.13.5 Redundancy and Availability

As shown on the figure above, an additional MDI is required for hot redundancy. The ASI switch detects the failure of a MDI and switches input to the redundant MDI. Therefore, both MDI must contain identical information.

4.4.13.6 Manageability

The SNMP Gateway allows an external system to read this module state and other basic information. See 4.4.22.

4.4.13.7 Failover Recovery

See 4.5.8.4.

4.4.13.8 Security

This section does not apply to this module.

4.4.13.9 Phoenix Customizations

This section does not apply to this module.

4.4.13.10 PHOENIX Customizations

This section does not apply to this module.

4.4.14 IMS database human data management tools

4.4.14.1 Description

A set of GUI applications enables the management of the IMS Database. They are used to perform the following tasks:

?? Product creation/modification

?? Schedule creation/modification

?? Network topology creation/modification

?? Blackout areas management

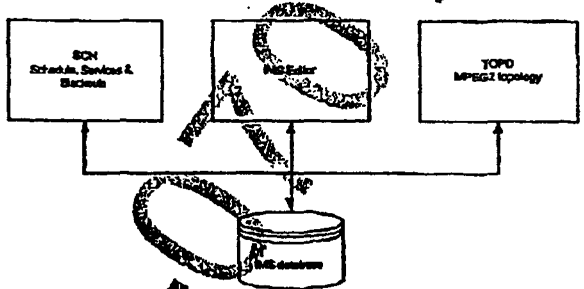

Figure 11 IMS database handling applications

4.4.14.2 Interfaces

This module offers a Windows graphical user interface.

4.4.14.3 Performance

This section does not apply to this module.

4.4.14.4 Scalability

This section does not apply to this module.

4.4.14.5 Redundancy and Availability

Redundancy is manual for interactive applications.

4.4.14.6 Manageability

This section does not apply for this interactive module.

4.4.14.7 Failover Recovery

This section does not apply to this module.

4.4.14.8 Security

Passwords are stored encrypted or not stored and asked at each application starting session.

Data transmission between the applications and the database are ciphered.

4.4.14.9 PHOENIX Customizations

This module will be customized for PHOENIX.

4.4.14.10 Topology Discovery (Top-D)

4.4.14.10.1 Description

Topology Discovery manages the network topology on the IMS Database. Standard feature of Top-D allows retrieving the transport configuration from the multiplexer. For Phoenix, it is mainly a monitoring tool.

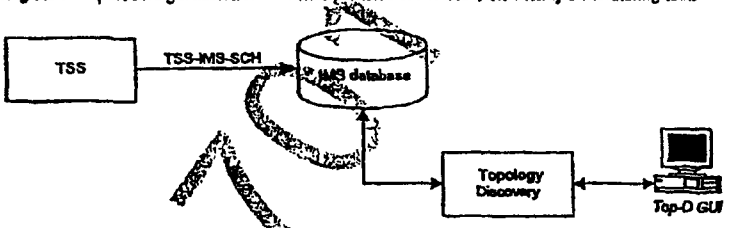

Figure 4.12

For a detailed description of Topology Discovery, see [TOPD].

4.4.14.10.2 Interfaces

See [TOPD].

4.4.14.10.3 Performance

See [TOPD].