

Every time the SMS gateway receives a product creation command, product data is sent to the product server. When the data defines a product that is an impulse PPV, then the IPPV server builds a message containing all necessary data to allow the SAS to create an EMM for impulse purchase (IEMM). The message is then sent to the SMS gateway.

### 3.3.10 ECM profile generator

The ECM profile generator is responsible for providing the SCS with the new ECM profile when a new event starts.

If multiple SCS are used, they are all connected to the same ECM profile generator.

An ECM profile describes the entitlements, which are required to be able to watch the event. Every time a new event starts, then a new profile is generated. For PPV events, there is usually a window at the start of the event during which the event is broadcast in free access mode. The duration of this window is usually set at the service level, but can also be set at the event level. In this case, the default value is overridden by the value specified at the event level.

The following table shows all the possibilities:

Access condition	Service level Condition value	Event level Condition value	ECM contents
Free access	No	No value	No
Free access	No	No	No
Free access	No	Yes	Yes
Free access	No	PPV	PPV
Free access	Yes	No value/Yes	Yes
Free access	Yes	No	No
Free access	Yes	PPV	PPV
Blackout	No	No value	No
Blackout	No	No	No
Blackout	No	Yes	Yes
Blackout	Yes	No value/Yes	Yes
Blackout	Yes	No	No

Usually, one ECM is required for each service. The elementary streams contained in the service can be of any type: video, audio, teletext, data, etc. They are all scrambled with the same control word.

Optionally, multiple ECMs can be required if different control words must be used. This is the case when different elementary streams must be sold separately. The NagraVision Pay-TV system provides up to 16 groups of streams that can be scrambled separately. This is far beyond the STB capabilities.

### 3.3.11 The Subscriber Authorization System (SAS)

The SAS is responsible for managing all the Entitlement Management Messages (EMMs) that have to be sent to each individual smartcard.

The SAS receives the EMM definitions from the various subsystems:

- ?? The SMS gateway
- ?? The IMS

Each EMM is encrypted by the EME and stored in the SAS database. The SAS determines when and for how long an EMM has to be broadcast: this is its EMM profile. The EMM and its profile are then sent to the EMM broadcaster.

CONFIDENTIAL

This document contains proprietary information of Kudatel SA which may not be further disseminated without the prior written approval of Kudatel SA.

**3.3.12 SAS functions**

The SAS manages all EMMs that have to be broadcast to the subscribers. It resolves any conflicts generated by contradictory EMMs (subscribe/unsubscribe, suspend/activate).

When it receives an EMM definition, the SAS gives the EMM to the EME for enciphering. Then it checks to see if there are contradictory EMMs already in its database. If so, these EMMs are removed from the database and the SAS also tells the EMB to stop broadcasting these EMMs.

When all the checks have been done, the EMM is sent to the EMB for broadcasting, together with a broadcasting profile. The profile indicates to the EMB how long and with what priority the EMM has to be broadcast.

**3.3.13 The EMM encryptor (EME)**

The EME is used to encipher EMMs. It also decipheres the EMM messages received from the STB during the callback to the call collector. Therefore, it is connected to the SAS and to the CC.

**3.3.14 The EMM broadcaster (EMB)**

The EMB continuously broadcasts EMM messages provided by the SAS. The EMB manages priorities and insures that all the EMMs are broadcast at regular intervals. The EMM queuing algorithm guarantees that a STB receives a maximum of 4 EMMs per second:

- ?? One EMM-U: a unique EMM, addressed to a given smartcard in a given STB.
- ?? One EMM-S: a shared EMM, addressed to a group of 256 smartcards.
- ?? One EMM-G: a global EMM, addressed to all smartcards.
- ?? One EMM-I: an impulse EMM, for impulse purchases (also called IEMM).

The EMB can broadcast up to 2000 EMMs per second. But this rate can be modified. Also, depending on the STB software and filtering capabilities, IEMMs can be broadcast as often as needed.

When the SAS sends a new EMM to the EMB, the EMM will almost immediately be broadcast. Then, depending on the number of EMMs and their repetition rate, it is broadcast again and again. The broadcasting period can vary from a few seconds to many hours.

Because each EMM is broadcast on all the streams transport on the network, the EMB is connected to all the MUX through an Ethernet connection. It is SNMP managed.

Optionally, the EMB can provide a Simulcrypt compatible stream.

**3.3.15 Call Collector (CC)**

The call collector manages the calls received from the STB. It has its own subscriber database that contains smartcard numbers and PPV information.

The STB calls the call collector when requested or at regular intervals to report the following information:

- ?? The list of PPV impulsively purchased
- ?? The current credit amount on the smartcard

The call collector registers this information and if necessary resets the credit limit on the smartcard. Then, it reports the list of PPV products to the SMS. With this information, the SMS is able to bill the subscriber.

The data transferred between the STB and the call collector is enciphered like EMMs. This insures a highly secure transmission. This is also the reason why the call collector needs an EME, in order to encipher and decipher the messages. A typical connection lasts approximately 30 seconds depending on the number of IPPV purchases to be reported, the speed of the modem and the conditions of the public network.

**3.3.15.1 Callback**

In general, the occurrence of a callback depends on the type of circumstances generating the callback. A callback belongs to one of three categories: automatic, on command, and event-based. In typical cases, callbacks will take approximately 30 seconds to complete full data transfer from the ICC to the CC.

**Automatic** - Automatic callbacks are strategically scheduled to occur during the night to minimize phone rates and phone line contention. These are setup at the Call Collector and may be scheduled by ICC UA.

**On Command** - On Command calls are generated for various reasons at the head-end site dependent on necessary conditions defined by the billing center. These callbacks will be performed immediately upon reception of the EMM generated by the SMS command 60. Callback data to the call collector will typically be received within 10 minutes after issuing the SMS command.

**Event based** - Event based callbacks occur as soon as one or more of the following conditions are satisfied:

- ?? **Threshold Limit** - The available credit falls below the threshold limit stored in the ICC. During this callback, expired PPV events (those whose end times are before the real time) will be reported. Credit is restored to the credit limit.
- ?? **Memory Full** - The ICC memory is full. Upon callback, the call collector will collect expired PPV events and send a reclaim memory command to the ICC. Credit is restored to the credit limit.
- ?? **Special Event** - A special event is an event defined as such by the SMS. When an event is defined as special, a callback will be triggered at the end of the event if the event has been watched (as defined by the watched flag in the smartcard) and impulsively purchased.

The following steps occur during the callback process (the order of the various steps may change):

- ?? Verify phone number if ANI enabled
- ?? Transfer current debit and credit data
- ?? Get list of expired impulsively purchased event products
- ?? Reset credit in the smartcard
- ?? Cleanup entitlements expired for more than 30 days.

CONFIDENTIAL

This document contains proprietary information of NagraVision SA which may neither be reproduced nor used in any form without the prior written approval of NagraVision SA.

© 1999 NagraVision S.A.  
CH-1033 CHESENAY SWITZERLAND

Page 22 of 123

Phoenix White Paper V10.doc

**3.4 Data inventory and bandwidth**

The following tables show the bandwidth required for each transport stream (TS) on a standard DVB system.

**PSI Information**

CAT	on every TS	15 Kbits/sec	
PAT	one per TS	30 Kbits/sec	
PMT	one per service	200 Kbits/sec	average of 10 services per TS

**DVB/SI information**

SDT actual & other	one per TS	100 Kbits/sec	average of 10 services per TS
NIT actual	on every TS	10 Kbits/sec	
EIT schedule	on one TS only	2 Mb/sec	500 services, 7 days EPG, period of 10 sec
EIT present/following actual & other	one per TS	100 Kbits/sec	
TDT	on every TS	1 Kbits/sec	

**Conditional access Information**

EMM	on every TS	100 Kb to 1 Mb/sec	depends of subscribers growth
ECM	on every TS	15 Kbits/sec per ECM	at least one ECM is required for every service
IEMM	on one TS for order ahead	110 Kbits/sec	period of 30 sec
IEMM	on every TS for current and next program	2 Kbits/sec/program	period of 1 sec

**3.4.1 EMM bandwidth calculation**

**3.4.1.1 Introduction**

The number of EMMs to be broadcast depends on the activity of the subscriber base. Daily operations include the following:

- Subscriber activations
- Subscriber deactivations
- Pay-per-view purchases
- Subscription updates

The number of EMMs needed is high during a period when the number of subscribers increases or decreases (churn) rapidly, but is much lower when subscriber movements are low, even if the number of customers is very high.

**3.4.1.2 Increase the number of subscribers**

To initialize each new subscriber properly requires about 10 EMMs to be generated. The initialization process includes sending entitlements, but also personal data like the postcode (zip code) or a credit for impulse purchases.

Subscription and initialization EMMs are broadcast for 2 days.

CONFIDENTIAL

This document contains proprietary information of NagraVision SA which may not be further disseminated without the prior written approval of NagraVision SA.

Number of new subscribers per day	Number of EMMs to be broadcast	Latency time for 750 Kbits/sec	Latency time for 100 Kbits/sec
500	10,000	10 sec	76 sec
1,000	20,000	20 sec	152 sec
2,000	40,000	40 sec	304 sec
4,000	80,000	80 sec	608 sec

Number of EMMs needed for 500 new subscribers =  $500 \times 10 = 5,000$ .

These EMMs are broadcast for 2 days; so the total number of EMMs in the EMM broadcaster =  $5,000 \times 2 = 10,000$ .

The latency time is the elapsed time between two broadcasts of any given specific EMM. We assume here that all the EMMs have the same priority.

**3.4.1.3 Update of Subscriptions**

These updates reflect the purchase of new products or the cancellation of products already purchased.

The calculations are based on the assumption that 1% of the subscribers will require 2 EMMs for modifying their product profile: one EMM for a new entitlement and another EMM to cancel an entitlement.

Day	Total number of subscribers	EMMs to update subscriptions (IEMMs)	Total number of EMMs for 2,000 new subscribers per day
1	2,000	0	20,000
2	4,000	40	40,040
3	6,000	120	40,120
4	8,000	200	40,200
5	10,000	280	40,280
30	60,000	1,140	41,140
60	120,000	2,340	42,340
90	180,000	3,540	43,540
360	720,000	14,340	54,340

**3.4.2 EMMs for Impulse purchase**

One EMM is needed for each PPV impulsively purchasable. This kind of EMM is called IEMM.

Assume that the number of PPV services is 50. The number of movie per service per day is 12 (one every 2 hour). The IEMM has to be broadcast for at least 7 days, which is the duration of the EPG grid displayed.

The total number of IEMMs =  $50 \times 12 \times 7 = 4200$ . In the context of the project Phoenix, they are broadcasted on a separate PID.

**3.4.3 Impulse purchase pay-per-view**

**3.4.3.1 Introduction**

Impulse purchase allows the subscriber to buy a product by means of the remote control of the STB only. The system can allow the impulse purchase of any kind of product, but it is mainly used for the impulsive purchase of Pay-Per-View movies.

One of the advantages of impulse purchase is that it is not necessary to call the SMS to order a movie. Nevertheless, it is always possible to order a movie by calling the SMS, even if it could be bought impulsively.

Impulse purchase is possible when:

CONFIDENTIAL

This document contains proprietary information of Kudoh SA which may not be further disseminated without the prior written approval of Kudoh SA.

7 19999 Nagravision S.A.

CH-1033 CHEVAUX SWITZERLAND

Page 24 of 223

File:WhitePaper\_VL.doc

- ?? The smartcard contains credit (money).
- ?? There is a method for regularly collecting the purchases in order to be able to bill the subscriber and to provide more credit on the smartcard.

Usually, credit is sent by means of EMMs and the collection is performed automatically via the telephone line. If no means of automatic collection is available, it is possible for the subscriber to bring his smartcard to a designated center where dedicated equipment can perform the collection and provide new credit.

### 3.4.3.2 System requirements

For every event (movie) that can be purchased impulsively, there must exist an IEMM that will be sent to the smartcard during the purchase process. This IEMM is broadcasted like EMMs, but on a separate PID.

When the subscriber wants to purchase a movie, the following actions happen:

- ?? The subscriber selects the grid guide option on the STB.
- ?? The events are displayed on the grid guide.
- ?? The subscriber navigates on the grid guide, examines the descriptions and selects the movie. A message like DO YOU WANT TO BUY THIS FILM appears.
- ?? The subscriber makes the purchase by pressing the YES key on the remote control.
- ?? The STB extracts the IEMM from the IEMM stream.
- ?? The IEMM is sent to the smartcard.
- ?? The smartcard deciphers the IEMM and extracts the price from the body of the IEMM.
- ?? The smartcard checks if enough credit is available. If so, the balance is updated and the subscription for the movie is stored on the smartcard.
- ?? The STB displays a message confirming that the movie has been purchased.

CONFIDENTIAL

This document contains proprietary information of NagraVision SA, which may not be further disseminated without the prior written approval of NagraVision SA.

1302 NagraVision S.A.  
CH-1033 CHESSALIX SWITZERLAND

Page 25 of 123

File: WhitePaper V1.0.doc

CV 2-07070

### 3.5 Geographical blackout description

To satisfy agreements with service providers or perhaps for legal reasons, some events should be available only in particular areas.

The NagraVision CA system offers this feature through a system of blackout types, normally related to the type of events (football, boxing...), and sub-types, related to areas where this type of event should be blacked out.

In other words, each type refers to a map and each subtype is a given area on the map. Since there are 12 maps available, there are 12 ways to organize these areas.

For every blackout type (numbered from 1 to 12), a particular smartcard belongs to one of 128 sub-types. Every event can belong to a blackout type and to a set of sub-types within this type. The smartcards that belong to one of the sub-types described in the event will be blacked out.

As an example, 3 blackout types can be defined as:

- ?? Type 1 (S): Blackout based on state  
Here each sub-type is the state number (in alphabetical order).  
This type of blackout is useful to satisfy state regulations.
- ?? Type 2 (B): Blackout on boxing events  
Here the sub-types are urban areas with boxing rings.
- ?? Type 3 (F): Blackout on football events  
Here the sub-types are urban areas with football stadiums.

The blackout information is sent to the smartcards by the mean of global EMMs. These are sent to all smartcards, but the EMM core contains the zip codes concerned by the blackout information. The smartcard will store the blackout information only if it belongs to one of the zip codes described.

The same mechanism is used for reverse blackout, or spot beam. Instead of describing areas where the access is forbidden, it describes only the areas where access is authorized.

CONFIDENTIAL

This document contains proprietary information of NagraVision SA, which may not be further disseminated without the prior written approval of NagraVision SA.

† 1569 NagraVision S.A. T  
CH-1033 CHESEBOLX SWITZERLAND

Page 28 of 123

File: WhitePaper-V1.0.doc

CN 2-2070





### 3.6 Products, entitlements and the smartcard database

#### 3.6.1 Access control

There are three types of access to programs:

- ?? Controlled access: the program is scrambled and the ECM has a specific access condition. Only smartcards entitled for this access condition will grant access to the program.
- ?? Free access: the program is scrambled, but the ECM has a free access condition, making valid smartcards to grant access unconditionally. Subscribers with no smartcard will not be able to watch the program.
- ?? Clear: unscrambled, unrestricted access with and without smartcard.

##### 3.6.1.1 Channel level access

The system is configured to give the same access condition to all programs on the channel. This is applied to channels like CNN. Blackout can be applied at the channel level.

##### 3.6.1.2 Program level

The system is configured to give different access conditions for each program broadcasted. This mode is usually applied to NVOD programs. Blackout can be applied to every program.

#### 3.6.2 Event profile definitions

On a TV service, events are identified by:

- ?? A starting date and time
- ?? A duration
- ?? A profile

The profile indicates:

- ?? A service number
- ?? A PPV number, for PPV events

The subscriber can watch the event only if he (or she) has purchased a product entitling him (or her) to watch. The entitlement will contain information like:

- ?? Start date: the starting date of the validity of the entitlement
- ?? End date: the ending date of the validity of the entitlement
- ?? Service number
- ?? PPV number: when the entitlement is related to PPV

Additional options allow access to be granted per theme (movie, news, children's programming, etc).

#### 3.6.3 ECM contents

The ECM is the Entitlement Control Message. It means that it contains information describing the profile of the event currently being broadcast:

- ?? Starting date and time of the event
- ?? Service number
- ?? PPV number (if a PPV event)

#### 3.6.4 Smartcard database

The smartcard contains records like a database. Every record is an entitlement containing the following fields:

- ?? Begin date    date of beginning of validity
- ?? End date      date of end of validity

CONFIDENTIAL

This document contains proprietary information of Nagra SA, which may not be further disseminated without the prior written approval of Nagra SA.

- ?? Service number
- ?? PPV number

All the records contained in the database represent all the authorizations granted to the subscriber. Subscriptions are managed by the means of EMMs.

### 3.6.5 Authorization verification

When an event is broadcast, an ECM is broadcast simultaneously. This ECM contains the profile of the event. This profile is matched against all the entitlements on the smartcard until one is found that grants access, or until all records have been checked. If no matching record is found, then watching that event is not permitted, the TV screen stays black and a suitable message such as ACCESS DENIED is displayed.

### 3.6.6 Service definition in the IMS

The IMS knows about the topology of the network. It means that it has to know all the service definitions.

A service definition contains the following data:

- ?? Service ID      The channel number visible to the subscriber. This can be changed at any time.
- ?? Transport ID    The transport stream on which it is transmitted
- ?? Service name    The name of the service

Example:

Service ID	Transport ID	Service name
35	1	CNN
36	1	CNN-FI
37	1	CNN-HEADLINE
50	2	HBO
51	2	HBO2
52	2	HBO3
60	3	ESPN
61	3	ESPN2
100	4	PPV 1 (a NVOD service)
101	4	PPV 2 (a NVOD service)

### 3.6.7 Products and entitlements in the IMS

In order to be able to send entitlements to a smartcard, they must be defined in the IMS. Entitlements can then be combined to build products: a product is a set of entitlements.

Because the memory space in the smartcard is limited, products must be defined and optimized to reduce the number of entitlements needed in the smartcard.

CONFIDENTIAL

This document contains proprietary information of NagraVision SA which may not be further disseminated without the prior written approval of NagraVision SA.

**3.6.7.1 Service related product examples**

Service related products grant access to one service or to a set of services for a certain period. The starting date of the period can be fixed or relative.

Examples:

- 1 year of CNN starting January 1 and finishing December 31
- 1 year of CNN starting July 1 and finishing June 30
- 1 year of CNN starting at any date and finishing 12 month later
- 1 year of CNN, MTV and CBS starting January 1 and finishing December 31
- 1 year of CNN, MTV and CBS starting July 1 and finishing June 30
- 1 year of CNN, MTV and CBS starting at any date and finishing 12 month later

**3.6.7.2 PPV related product examples**

PPV related products grant access to one PPV or to a set of PPVs.

Examples:

- |                                    |                                   |
|------------------------------------|-----------------------------------|
| The Super Bowl on ESPN             | one PPV event only                |
| One year of ESPN                   | all PPV on ESPN for one year      |
| Titanic                            | one PPV movie only                |
| The Clint Eastwood Movies package  | 10 movies with Clint Eastwood     |
| The best of Hitchcock for 6 months | all Hitchcock movies for 6 months |

In the current DVB implementation, only products related to one PPV are impulsively purchasable. All the other products must be ordered by calling the SMS center. An impulsively purchasable product can also be ordered by calling the SMS center.

CONFIDENTIAL

CV 2-07010

CONFIDENTIAL

This document contains proprietary information of Kudoh SA which may not be further disseminated without the prior written approval of Kudoh SA.

1998 Nagravision S.A.   
 CH-1033 Cheseaux, SWITZERLAND

Page 30 of 123

File: WhitePaper\_V1.0.doc

### 3.7 Current Phoenix system components functional description

#### 3.7.1 Billing system

The billing system is responsible for managing subscriber profiles, billing, etc.

#### 3.7.2 APC/IR

The APC/IR is responsible for the physical connection to the CAMC and the association between subscriber ID and the smartcard number.

#### 3.7.3 Traffic and scheduling system (TSS)

Central repository for all scheduling information.

#### 3.7.4 Broadcast control system (BCS)

Interface to the various automated systems (Drake, Philips, etc).

#### 3.7.5 SDDS

Almost real-time module providing information to the online equipment.

#### 3.7.6 Advanced program guide (APG)

Advanced program guide stream generator. It receives information from the TSS and builds an appropriate formatted stream.

#### 3.7.7 CAMC

Generates conditional access packets.

#### 3.7.8 CAUS

Generates control words packets and its content.

#### 3.7.9 USPS

All the equipment for encoding, multiplexing and modulation.

CONFIDENTIAL

This document contains proprietary information of Kudatell SA which may not be further disseminated without the prior written approval of Kudatell SA.

© 1999 NagraVision S.A.   
 CH-1033 CHEVAUX SWITZERLAND

Page 31 of 123

File: WhitePaper\_V1.0.doc

**3.8 Existing system components modifications**

**3.8.1 Billing system**

If hand pairing between the IRD and the smartcard is required, the billing system shall manage the IRD serial number

**3.8.2 APC / IR**

Same requirements as for the billing system.

**3.8.3 Traffic & scheduling system**

Interfaces to the IMS must be created and the TSS must manage NagraVision CAS related data.

**3.8.4 SDDS**

Last minute change interface to the IMS and user interface for the NagraVision CAS data must be created.

**3.8.5 Advanced program guide (APG)**

APG must contain the PID Information for the additional EMM, IEMM and ECM streams.

**3.8.6 IRD**

Requires different filtering configuration and more Mpeg-2 oriented mechanisms. IRD code download specifications must be verified in order to make sure that the download stream is authenticated and is appropriately selected by the IRD.

**3.8.7 CAM**

Existing NagraVision CAM Rom Code will be modified to satisfy specific Phoenix requirements.

**3.9 New system components**

**3.9.1 CAS translator & router**

This module will route the BS commands to and from the appropriate CAS, depending on the smrand number. It will also translate the current BS commands into SMS Gateway commands.

**3.9.2 Control word distributor**

This module will extract the control word provided by the CAUS and send it to the SCS. Simultaneously, it will send the CW and CWP untouched to the multiplexer.

CV 2-07070 ABC CHH

HIGHLY CONFIDENTIAL

**3.10 System interfaces**

**3.10.1 Introduction**

The interfaces can be classified in the following categories:

- ?? The interfaces that are open standards
- ?? The interfaces defined by NagraVision and that will be used as is
- ?? The interfaces either defined by Phoenix/NagraVision or not existing that will be designed

All interfaces between the system components of Figure 1 - Phoenix-NV Head-end architecture are network centric interfaces based on open OSI communication standards such as Ethernet and TCP/IP. Stars identify the interfaces between the NagraVision components and the existing Phoenix system.

The interface are named and their functions outlined here below:

Interface number	Interface name	Data transferred	Function description	Specification status
1	SMS Gateway	SMS Gateway commands	Open interface to the NagraVision CAS	Available by NagraVision
2	TSS-IMS-SCH	Scheduled and transport configuration (topology)	Provide all the program scheduling information and the PID (SCID) configuration	To be specified
3	TSS-IMS-DES	NagraVision private descriptors	NagraVision conditional access related information, for APG customization and impulse purchase	To be specified
4	TSS-IMS-PRD	Product definition	Each product known by the TSS is mapped into the NagraVision equivalent product	To be specified
5	SDDS-IMS-LMC	Last minute change	Inform IMS about last minute changes, in order to provide the appropriate ECM profile in the ECM	To be specified
6	CWD-SCS-CW	Control word	Provide the control word to the SCS, in order to put it in the ECM	To be specified
7	MDH-MUX	ECM, EMM and IEMM	Inject EMM, ECM and IEMM into the transport stream	Content definition available, physical interface DVB standard

**3.10.1.1 DSS versus MPEG2**

MPEG-2 packets required by the current NagraVision system are converted into DSS packets. The only difference is the length of the packet. The content of the DSS packets for the NagraVision PID stays similar to MPEG-2 tables and sections.

**3.10.2 Standard interfaces**

**3.10.2.1 DVB-Simulcrypt**

This protocol is described in [DVB\_SIMUL]. It describes the interface between the CAS and the multiplexer for EMM and ECM injection. Most manufacturers and CAS providers implement it.

CONFIDENTIAL