NAGRAVISION®

DIGITAL PAY-TV SYSTEMS

Confidential

IRD MASTER/SLAVE

Implementation Guideline

ISSUE 0.0.3

First published, March 2003.
Revised,.
Last printed: 27 May 2003
Part number: IRD Master_Slave Implementation_Guideline v0.0.3.doc

Nagravision S.A. is a member of the Kudelski Group of Companies.
Tel.: (41) (21) 732-0311 Fax: (41) (21) 732-0300

Security Policy of Nagravision S.A. (Kudelski Group)

Any recipient of this document, without exception is subject to a

Non Disclosure Agreement (NDA) of Nagravision S.A. (Kudelski Group) prior to delivery.

Contents

List of Tables

List of Figures

Acknowledgements

Printing or viewing online

NOTICE It is strictly prohibited to print this document if it is marked "Online use only" or to disseminate this document with a screen dump/capture utility or similar tool or to view it on a machine that is not part of the System that it was supplied for use on.

This document is supplied with a strict understanding that the notice(s) herein or any other contractual agreement(s) made that instigated the delivery of a hard copy, electronic copy, facsimile, file transfer, any other means to hardcopy or transfer this document are strictly observed and maintained.

This document is supplied in Portable Document Format (PDF) format and it requires Adobe Acrobat Reader 3.0 (or later) to be printed (or viewed online). It is recommended to print this document double-sided on A4 paper (Also see note) using a laser printer. If your printer does not have double-sided mode—See your printer's documentation.

Note To print on letter size paper, in Acrobat reader, click **Print…** from the **file** menu (Print dialogue box appears), and then select **shrink to fit** check box.

Acronyms and Abbreviations

Term	Definition	Description
BSA	Black screen mode active	The STB is locked and a black screen (with an information panel) is shown.
CME	Continuous mode enabled	The slave STB is running using the continuous mode
CM/S	Check Master/Slave	The validation procedure is active
DVB	Digital Video Broadcasting	DVB is a family of international standards for all program delivery media: satellite, cable, terrestrial, microwave, MDS, CATV, and SMATV.
EMM	Entitlement Management Message	Conditional Access message sent to the smart card in order to set, reset or change private access rights, credit etc.
ICC		Smart card.
NoM/S	No Master/Slave mode enabled	The Master/Slave mode is disabled on the STB
SSME	Single Shot mode enabled	The slave STB is running using the single shot mode.
STB	Set Top Box	Interface device that allows receiving signal, demodulates it and de-scrambles it.

Table 1 - Acronyms and Abbreviations

Reference

[1] NagraVision, Set-Top Box & Multimedia, Conditional Access Kernel, Overview, V 1.5.0 or later
[2] NagraVision, Set-Top Box & Multimedia, Conditional Access Kernel, Application Programming Interface, V 2.2.2 or later
[3] Nagravision, Digital Terminal Division, Conditional Access Kernel, IRD Commands specification, v1.3.x or later.

1. Introduction

1.1. Objectives

The objective of this document is to describe how to implement the IRD Master/Slave solution in the STB. The IRD Master/Slave solution is managed by the STB. Nagravision manages the initialisation and configuration of the IRD Master/Slave solution using the IRD commands. Please refer to [1] for a presentation of the CAK in general and of the IRD command mechanism in particular. Also see [3] for details about the format of the IRD Master/Slave IRD commands. The IRD commands are defined in the present for information. The only reference for these commands is [3].

1.2. The document structure

In the §2, all IRD commands used to implement the IRD Master/Slave solution are defined here for information. Some explanations of the goal of some parameters are also added, as well as an implementation guideline for every IRD commands is included (not only the IRD Master/Slave commands).
In the §3, the behaviour of the IRD Master/Slave system will be clarified. A state machine will be used to describe the process.

1.3. Overview

The IRD Master/Slave functionality is designed to prevent loss of revenue in the situation that an operator provides a slave STB and subscriptions to a subscriber at a lower cost but the slave STB is then transported to a separate dwelling or location. The concern for operators is to prevent the move of slave to a separate dwelling or location. Therefore the IRD Master/Slave solution makes the move of slave to a separate dwelling or location much more difficult by forcing the subscriber to regularly insert the Master smart card into the slave STBs, called the validation procedure.
This system has two modes:

- The continuous mode
- The single shot mode

A brief reminder of the behaviour of these modes follow.

1.3.1. Continuous mode

The continuous mode is initialised once by the SMS. Each time the validation of the slave STB is done by inserting the Master Smartcard, the STB calculate the next validation date. The procedure is fully managed by the STB. The time to the next validation is called ‘validationTarget’. The average number of days between two validations is the ‘validation period’. Once the validation procedure is stated, the ‘timeout’ define the period of time that the customer has to insert the master Smartcard in the slave STB.
In order to have a validation period not too regular another parameter is inserted: the ‘random period’. The parameter defines a window of time with the validation delay as follow:

- Lower window limit: ‘validation period’ – ‘random period’
- Upper window limit: ‘validation period’ + ‘random period’

The STB define randomly the validation target within this window. Of course, the random period must be lower or equal to the validation period.
For example: If the validation period is 7 days, the random period is 2 day; the next validation target will be in 5 to 9 day for a ‘timeout’ period of time.

1.3.2. Single shot mode

In the single shot mode, the validation procedure begins directly after the initialisation command arrived. If no Master Smartcard insertion occurs, the black screen is displayed after ‘timeout’ hours. If the single shot initialisation command occurs when the continuous mode is running, the single shot is executed. After the successful end of the validation procedure for the single shot, a new validation target date is calculated by the STB for the continuous mode.

2. IRD Commands

Three IRD commands are defined for that purpose:

- Continuous mode initialisation command
- Cancellation command
- Single shot command

The IRD commands are defined in [3], the following values are for information only. The command_id (see [3]) for all the following command is 0xC7. The operation (see [3]) will increase for each following commands as described in the following table.

Name	command_id	operation
Master/Slave continuous mode initialisation	0xC7	0x01
Master/Slave cancellation	0xC7	0x02
Master/Slave single shot	0xC7	0x03

Table 2 - Commands Summary

2.1. Continuous mode initialisation command

This command is used to set the parameters in order to initialise the Master/Slave continuous mode. The parameters are explained in there descriptions.

Format

```
IRD_command(){
  EMM_command              8    uimsbf     value 0x64
  length                   8    uimsbf     value = 14
  command_body{
    sequence_number        32   uimsbf
    command_id             8    uimsbf     value 0xC7
    operation              8    uimsbf     value 1
    data {
      masterSmartcard      32   uimsbf
      validationPeriod     8    uimsbf     in days
      randomPeriod         8    uimsbf     in days
      timeout              8    uimsbf     in hours
    }
    checksum               8    bslbf
  }
}
```

Parameters

`sequence_number`	value incrementing with each command. Command with the same sequence number is processed only once.
`command_id`	command identifier number, described in the next sections.
`operation`	used in conjunction with the command_id. The couple (command_id, operation) uniquely identifies a command.
`masterSmartcard`	this is the Smartcard ID of the master Smartcard without checksum.
`validationPeriod`	this value define the average time, expressed in days, between two validation procedures.
`randomPeriod`	the next validation procedure will occur in `validationPeriod` days +/- `randomPeriod` days. The targeted day will be randomly chosen in this bracket of time.
`timeout`	the timeout is the period of time during which the customer has to succeed with the validation procedure (insert the master Smartcard in the slave STB). At the end of the `timeout` period, the STB will stop playing video and/or audio signal.
`checksum`	two's complement of the sum of all bytes from the command_id to the last data byte. The sum of all bytes from the command_id to the checksum must be equal to 0.

2.2. Cancellation command

This command id used to disable the IRD Master/Slave mode continuous and single shot mode. The operation of the command is 2.

Format

```
IRD_command(){
  EMM_command           8    uimsbf     value 0x64
  length                8    uimsbf     value = 7
  command_body{
    sequence_number     32   uimsbf
    command_id          8    uimsbf     value 0xC7
    operation           8    uimsbf     value 2
    data {
                                        no data in this command
    }
    checksum            8    bslbf      value 0x37
  }
}
```

Parameters

`sequence_number`	value incrementing with each command. Command with the same sequence number is processed only once.
`command_id`	command identifier number, described in the next sections.
`operation`	used in conjunction with the command_id. The couple (command_id, operation) uniquely identifies a command.
`checksum`	two's complement of the sum of all bytes from the command_id to the last data byte. The sum of all bytes from the command_id to the checksum must be equal to 0.

2.3. Single shot command

This command is used to set the parameters in order to initialise the single shot Master/Slave command. This is not possible to disable this command only; all Master/Slave modes must be disabled in order to cancel it. In other words, it's not possible to cancel a single shot command without cancelling the continuous mode. The operation of the command is 3.

Format

```
IRD_command(){
  EMM_command            8    uimsbf     value 0x64
  length                 8    uimsbf     value = 7
  command_body{
    sequence_number      32   uimsbf
    command_id           8    uimsbf     value 0xC7
    operation            8    uimsbf     value 3
    data {
      masterSmartcard    32   uimsbf
      timeout            8    uimsbf     in hours
    }
    checksum             8    bslbf
  }
}
```

Parameters

`sequence_number`	value incrementing with each command. Command with the same sequence number is processed only once.
`command_id`	command identifier number, described in the next sections.
`operation`	used in conjunction with the command_id. The couple (command_id, operation) uniquely identifies a command.
`masterSmartcard`	this is the Smartcard ID of the master Smartcard without checksum.
`timeout`	the timeout is the period of time during which the customer has to succeed with the validation procedure (insert the master Smartcard in the slave STB). At the end of the `timeout` period, the STB will stop playing video and audio signal.
`checksum`	two's complement of the sum of all bytes from the command_id to the last data byte. The sum of all bytes from the command_id to the checksum must be equal to 0.

2.4. IRD Implementation Guidelines

The implementation of the IRD Master/Slave feature relies on functions provided by the CAK API; see [2].

2.4.1. Upon Initialisation

During its initialisation phase, the set-top box software has to register callback functions with the CAK in order to enable several CAK features. The IRD command mechanism requires such a registration. The function to use is `caRegisterIrdCmdExportation()`. When calling this function, the set-top box software registers a callback function that will get called by the CAK every time an IRD command is received. NagraVision specifies the prototype of this callback function. Please refer to [2] for details.

2.4.2. Upon Reception of an IRD Command

The very first thing the IRD command callback function shall do when it gets called (once initialised), is to copy the IRD command's data into a buffer of its own, then acknowledge the CAK using the acknowledgement callback function (provided by the CAK as a parameter). The buffer provided by the CAK will be freed by the CAK just after the acknowledgement. For details about this acknowledgement mechanism, please refer to [2]. The IRD command callback function's next job is to process the command according the IRD command's `command_id` and `operation` fields. These fields are used to distinguish amongst the various types of IRD command.

2.4.3. Processing of an IRD Command

An IRD command is included in an EMM. Remember that the EMM is broadcast in loop for a given time. The EMM catch the STB maybe every 10min until the end of its life. At this stage, the `sequence_number` field of the IRD command shall be taken into consideration to determine if this is a new IRD command or the same IRD command broadcast once again. A variable shall be used for each kind of IRD command (3 in the IRD Master/Slave solution). This variable, let's name it with a very explicit name for the purpose of this

explanation, say, `sequenceNumbersProcessedFIFO`, shall be an array of 16 unsigned 32-bit integers (to store the 16th last `sequence_number` processed of this IRD command.
By using this variable, it is possible for the set-top box software to determine whether it's a newly received IRD command or the same command as the previous one, broadcast once again. However, to allow the set-top box to keep the 16 last processed command and yet not re-process it after a reset of the STB, it is necessary for this variable to be stored in non-volatile memory. The initial values of `sequenceNumbersProcessedFIFO` do not matter, but the value of all fields must be the same. Table 3 on page 9 shows a code abstract that illustrates how to determine if the IRD command is already processed.

```
...
#define SEQUENCE_NUMBERS_PROCESSED_SIZE 16
...
if ((command_id == MyIRDCommand) && (operation == MyOperation)) {

       /* Check whether the newly received IRD command */
       for ( int i = 0; i < SEQUENCE_NUMBERS_PROCESSED_SIZE; i++ )
              if ( newlyReceivedSequenceNumber == sequenceNumbersProcessedFIFO[ i ] )
                     return; /* IRD command must be ignored. */

/* IRD command must be processed. */
/* The sequence_number must be store if the command is successfully executed */
}
...
```

Table 3 – Check the new Sequence Number

Then the IRD command must be executed. Once the process of the command is completed and successful, the last used `sequence_number` must be store in a `sequenceNumbersProcessedFIFO`.

```
...
/* The IRD command is processed successfully. */

/* Record the sequence number already processed. */

for ( i = 0; i < SEQUENCE_NUMBER_PROCESSED_SIZE - 1; i ++ )
       sequenceNumbersProcessedFIFO[ i ] = sequenceNumbersProcessedFIFO[ i + 1 ];
sequenceNumbersProcessedFIFO[ i ] = newlyReceivedSequenceNumber;

/* END of process */
...
```

Table 4 – Storing the Sequence Number

As already said, the process must be done separately for each IRD command (Master/Slave commands or not).

3. IRD Master/Slave principles

3.1. State machines of the IRD Master/Slave system

One state machine is necessary to describe the IRD Master/Slave solution. In the solution two modes are possible:

- The continuous mode
- The single shot mode, that have the priority

The five possible states of the machines are:

- No Master/Slave mode enabled (NoM/S)
- Continuous mode enabled (CME)
- Single shot mode enabled (SSME)
- Check the Master/Slave (validation procedure) (CM/S)
- Black screen mode active (BSA)

The transitions are:

- Init continuous mode (using the continuous mode initialisation command: 0xC7/1)
- Clear continuous mode (using the continuous mode cancellation command: 0xC7/2)
- Enable single shot mode (using the single shot command: 0xC7/3), the previous state of the command must be saved in order to return to it after succeeded with the validation procedure. The two possible saved state are NoM/S & CME.
- Validation procedure (Automatic according to the IRD Master/Slave parameters)
- Timeout (Automatic if no check is successful during period)
- Master SC inserted; the machine return to the previous state

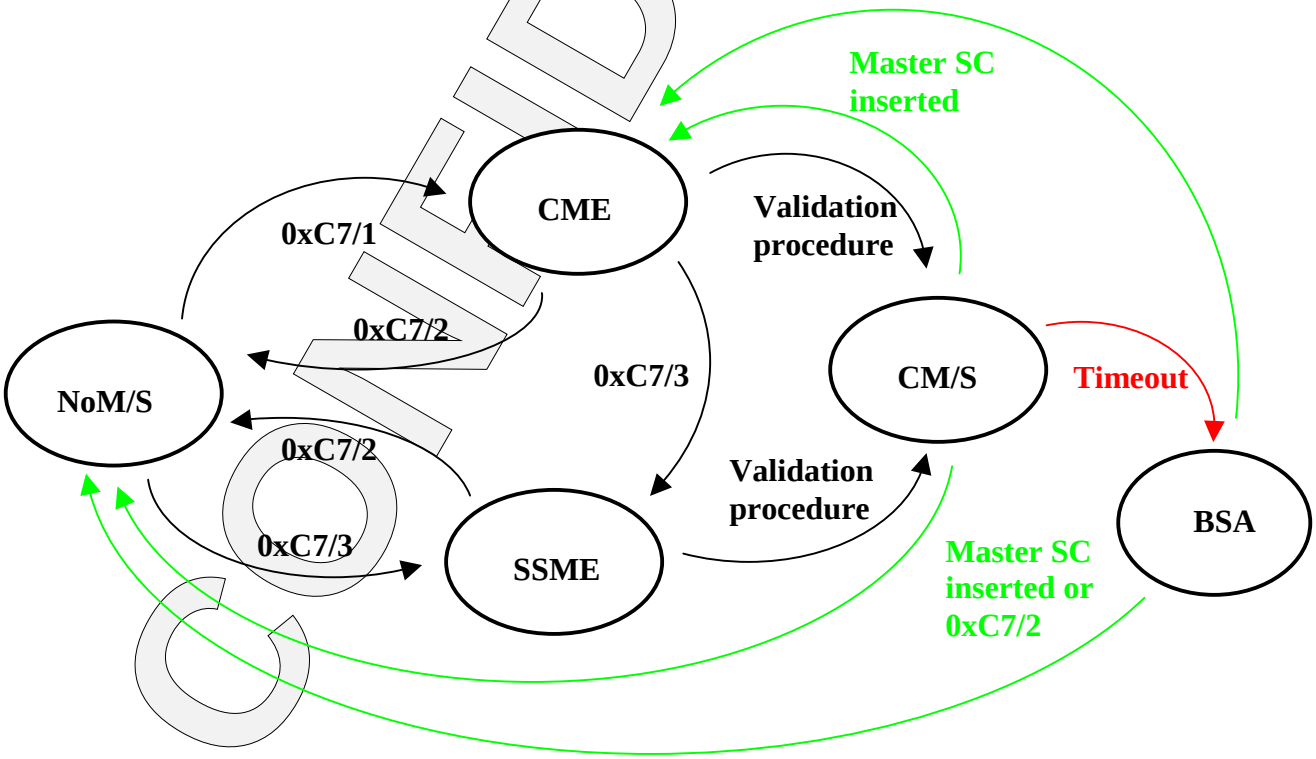

Figure 1 – Master/Slave IRD command state machine