NAGRAVISION®
DIGITAL PAY-TV SYSTEMS

CONFIDENTIAL

IRD MASTER/SLAVE

Solution Overview

ISSUE 1.0.0

Contents

Nagravision S.A., CH–1033 Cheseaux, Switzerland
Tel : +41 21 732 0311, Fax:+41 21 732 0300, Web: www.nagra.com

1. Introduction

Having multiple Set Top Boxes (STB) in the same home is already common in the United States and is getting increasingly frequent in Asia and Europe. The STBs are referred to as Master and slave. Homes with a single STB only have a Master. Additional STB in the same home are slaves. Given the STBs are identical as is the network feed, it is easy to carry a STB from one home to an other. So one entrepreneurial subscriber could have friends benefit from his reported slaves STBs. He could even re-sell the slave subscriptions for a profit by creating a commercial pirate slave network.

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. In fact, the concern for operators is to prevent the move of slave to a separate dwelling or location.

1.1 Document history

Version	Date	Author	Description
1.0	2003-05-07	Marc Uldry	First version.

1.2 References

[1] IRD Master/Slave Implementation Guideline, v0.0.3, Nagravision

[2] IRD Commands specification, v1.3.x or later, Nagravision

2. IRD Command

The IRD commands allow the head-end to send messages to the set-top box in a secured way. IRD commands are carried by EMMs and therefore benefit from EMM addressing mode. It means that a message can be addressed to one single set-top box or in the opposite to all set-top boxes.

The CA Kernel embedded in the set-top box is not dependent at all on IRD commands. It gets the command from the smartcard and forward it to the set-top box application without additional processing. The set-top box application is completely responsible of IRD command management. Please refer to [2] for details about IRD commands.

3. IRD Master/Slave solution

The proposed 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.

The SMS sends to the slave STBs an IRD command to trigger a revalidation with the Master smart card. Upon reception of this command, the slave STB:

- → Executes the command and sets up internal deadline time,
- → Prompts subscriber to insert the Master smart card within specified deadline,
- → Brings up promt upon command execution and subsequent exit from stand-by mode, and
- → Blocks access to signal if the Master smart card is not inserted in due time.

Two different modes, as described below, can be applicable, either separately or concurrently.

3.1 Single shot mode

In the single shot mode, an IRD command is sent periodically to a slave STB to trigger immediate revalidation from the Master smart card. In this mode, the IRD command carries:

- The ID of the Master smart card, and
- The amount of time until cutoff.

The subscriber is prompted to insert the Master smart card during the amount of time until cutoff.

3.2 Continuous mode

In the continuous mode, an IRD command is sent once to a slave STB which then automatically triggers revalidations from the Master smart card at regular intervals. In this mode, the IRD command carries:

- The ID of the Master smart card,
- The amount of time until cutoff,
- The number of days between revalidations, and
- A value in order to randomly modify the the number of days between revalidations.

The subscriber is prompted to insert the Master smart card during the amount of time until cutoff.

4. Uses cases

4.1 Single shot mode

A slave STB receives, from the SMS, an IRD command with a time to cutoff equal to 48 hours. Upon command reception, the slave STB prompts right away to insert the Master smart card. This message is prompted again every time the slave STB exits from the stand-by mode.

In the case the subscriber inserts the Master smart card into the slave STB within 48 hours, the slave STB is revalidated *until next command is received.*

In the case the subscriber does not insert the Master smart card into the slave STB within 48 hours, the slave STB cuts access to signal until Master smart card is inserted.

4.2 Continuous mode

A slave STB receives, from the SMS, an IRD command with a time to cutoff equal to 24 hours and with a number of days between revalidation equal to 7 days. Upon command reception, the slave STB prompts right away to insert the Master smart card. This message is prompted again every time the slave STB exits from the stand-by mode.

In the case the subscriber inserts the Master smart card into the slave STB within 24 hours, the slave STB is revalidated for 7 days and will launch *automatically* revalidation request thereafter.

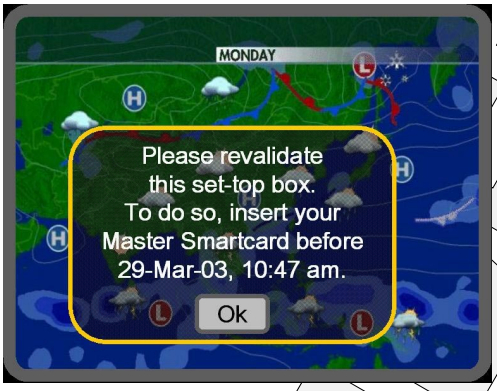
In the case the subscriber does not insert the Master smart card into the slave STB within 24 hours, the slave STB cuts access to signal until Master smart card is inserted.

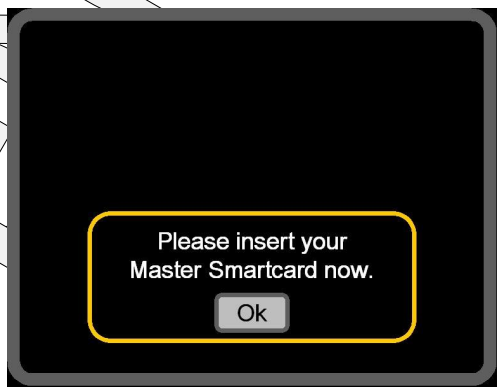
5. Storyboards

The following pictures give examples of messages that the slave STB could prompt on different situations.

5.1 With revalidation in time

Either in the continuous or in the single shot mode, the subscriber is prompted to insert the Master smart card during the amount of time until cutoff. The subscriber must then remove the slave smart card (i.e. with intent to insert the Master smart card instead).

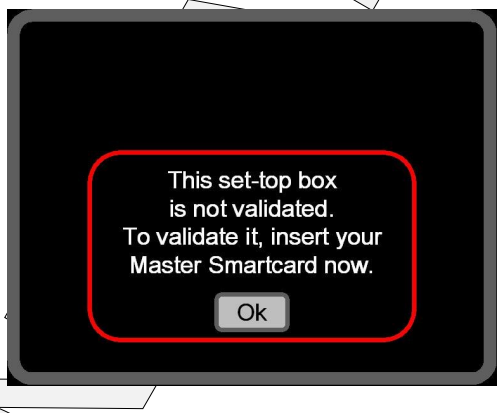




Once the slave smart card removed, the subscriber must insert the Master smart card in order to revalidate the STB. The subscriber can then re-insert his initial slave smart card, and continue to watch TV.

5.2 Without revalidation in time

Either in the continuous or in the single shot mode, the subscriber is prompted to insert the Master smart card during the amount of time until cutoff. In the case the subscriber does not insert the Master smart card into the slave STB within time to cutoff, the slave STB cuts access to signal until Master smart card is inserted.



However, once the slave smart card removed and the Master smart card inserted for revalidation, the subscriber can continue to watch TV.

6. Limitations

The IRD Master/Slave solution has the main advantage of being easy to deploy and to manage from a PayTV operator's point of view, but requires a strong collaboration from the set-top box manufacturer.

In fact, as mentionned in the section 2, the Master/Slave IRD commands are carried by means of EMMs. This mechanism allows the head-end to send messages to the set-top box in a secured way as the EMMs are encrypted. Only a valid smart card can decrypt those IRD commands, which are then forwarded in clear to the set-top box application. From that point onwards, the set-top box application is responsible for the IRD commands and its content.

Although not fully resistant to "professional attacks", this first level of security will prevent "Mr. Everybody" to take advantage of the system. In case a higher security is needed, Nagravision would be pleased to discuss an extension towards a more secure solutions.

—— END OF DOCUMENT ——