WWW.MAESTRA.CA

For the latest satellite testing file & software releases. Bell ExpressVu & Dish Network Keys in Real Time!
INTRODUCTION:

We are now at version 5 of the guide. Originally this reference manual was published with newbies in mind but has since evolved into a tool used by all satellite testers. Included in this guide are all the possibilities offered to the testing community as of its publishing. As always, your questions, comments and technical input are welcomed in order to maintain this fantastic manual updated.

TERMS AND ABBREVIATIONS:

8515
Short for the ATMEL AT90S8515 microprocessor used on the AVR

Access Card – see also CAM

It is also called the Smartcard. This card can be taken out of the receiver (IRD) and interacts with the data sent from the satellite feed. It allows the channels you pay for to be unscrambled and is used to program your receiver. Pay per view (PPV) data is stored in this card.

Activation

Procedure by which the user subscribes to a programming package with a Satellite provider to activate his receiver. This provider in turn sends a signal through the satellite feed to the subscriber’s receiver that contains all the information of the receiver and what the subscriber has asked for and purchased in his package which match what is on the CAM. From this point on the CAM is “married” to the receiver.

Antenna or dish

Device used to capture the satellite signal and sending it to the receiver using a coaxial cable.

ATMEGA

Microprocessor manufactured by the Atmel Corporation. This chip is used on the new generation Atmega128 and EFA-Atmega boards.

ATMEL

Manufacturer of microprocessors (AT90, Atmega etc.)
**ATR**

"Answer to reset" Each time your CAM is activated or reset it must send data to the receiver (IRD) so it can determine the needs of the CAM (Communication protocol, voltage etc.) The ATR allows the CAM to send to the receiver (IRD) the right polarity to use, the number of bauds for the transmission etc.

**Autoroll**

When the CAM or an electronic card (like an AVR) has the ability to get the public key which it needs on its own from the service provider’s signal it is then considered an Autoroll card.

**AVR**

AVR Terms such as "Audio Video Replicator" have been used to describe an AVR. AVRs exist in many "flavours" such as:

**AVR1:** The AVR1 is a plastic circuit board (PCB) with one ATMEL AT90S8515. This type of card has no DB25 connector and no ISO 7816 connector. To program it you need an external programmer.

**AVR2:** Same as AVR1 except that you have one DB25 connector to plug into your computer’s parallel port in order to program it.

**AVR3:** Same as the AVR2 plus an ISO 7816 connector (or slot) to insert your real CAM.

**AVR4:** It’s essentially an AVR3 with jumpered pins 10 and 12 of the Atmel in the DIP type or the 11 and 14 pins in the case of the PLCC.

**AVR5, AVR6:** These terms are mostly used by dealers, in reality they are AVR3s with the jumpers. Dealers introduced these cards with different designations to distinguish cards that use one more electronic chip that gives the card the Autoroll function or a different kind of presentation (wafer card).

**Baseband**

Name given to the brut signal emitted by the satellite before it is demodulated by the receiver (IRD) so it can be viewed on a television set.

**BEV**

Bell ExpressVu

**Blockers**

Procedure to prevent Electronic Counter Measures sent down by the provider. These blockers are either mechanical (installed in the IRD) or programmed on a ROM2 or ROM3 card to prevent a system failure during ECM’s.

**Bootstrap**

The bootstrap is the master program that runs the CAM, AVR or Atmega. Without the bootstrap they become impossible to use. The "bootstrap" is generally not accessible by the public.

**Boxkey**

Represents a unique IRD number and is used to generate the private decryption key in the satellite data feed. This number is written to the TSOP of the IRD.
**CAM – Conditional Access Module**

Also called the Smartcard. This card can be removed from the IRD and interacts with the signal emitted by the satellite and in return allows the IRD to be programmed. Again here there are different types of CAMs:

**ROM2:** This type of card (relatively old) can be reprogrammed in an ISO programmer to receive every channel without the use of an AVR or Atmega board.

**ROM3:** This card replaced the ROM2 for security reasons. It was also reprogrammable in the same way as the ROM2 due to a malfunction called a “back-door”. These were locked by an ECM in July 2001. The ROM3 cards that were not affected by this ECM are called “open” and can be reprogrammed. It is possible to “reopen” a card that has been closed by the ECM but usually dealers and experts do this at great cost. This function will be explained further into this manual.

**ROM7:** Model used exclusively by BEV which can not be reprogrammed.

**ROM10:** Used to replace ROM3 and ROM7. Again this card is not reprogrammable.

To determine which type of card you have:
- Put the CAM in the receiver and power on;
- On the remote hit SysInfo;
- You will see a window with this information:

**MODEL ID:** 2700 (or the one you have)
**RECEIVER CA ID:** R00xxxxxxxx-xx
**SMARTCARD CA ID:** S0xxxxxxxx-xx
(Card ROM version) => DNASP003 Rev xxx <= software version

**DNASP003** represents a ROM3 card type A2012 or 288-02 these are programmable (if they were not hit by the ECM of July 2001) or can be fixed.
**DNASP002** represents a ROM2 card type – 288-01. This card is programmable but can not be fixed.
**DNASP010** represents a ROM10 card type. This card is not programmable and can not be fixed.

**CAM ID#**

Serial number written on the CAM, this number starts with S00...

**CEMU**

Name given to the computer emulation software running under DOS.

**Downlink**

Data feed from the satellite to the dish.

**Dump**

Procedure that allows a processor to download to a software all of the data contained in its memory chip.
**E3M**

Also known as "Echostar/Dishnetwork 3M". This card unscrambles all channels including PPV on the Echostar/dishnetwork system. An AVR has a similar function on the BEV system. If this card has the means of updating itself to the new keys from the provider’s signal, it is then called Autoroll.

**ECM – Electronic Counter Measures**

Used to render illegal devices inoperable. In fact this is a command transmitted in the data stream to detect any illegal devices attached to the receiver and to put these devices out of order. It can also rewrite the TSOP or EEPROM and cause the receiver to become inoperable. ECMs are emitted without prior notice.

**EEPROM**

"Electronically Erasable Programmable Read Only Memory". The EEPROM is an electronic chip that can be read or written to. It is widely used, for example, in the IRD for storage of information relative to your favourite channels, language etc...

**EFA-Atmega**

Name given by its creator (Omega) to the new generation of AVRs. This new board is equipped with an Atmega128 microprocessor manufactured by the Atmel Corporation. This board is considered to be original while other models available on the market are clones. Only original "Omega" designs are named EFA-ATMEGA.

**Emulator**

Device and software used to emulate the original functions of the CAM.

**EVU**

Bell ExpressVu

**IRD - (Integrated Receiver Decoder)**

Receiver of signals emitted by a satellite. The receiver has an integrated demodulator making it possible to receive a "rough" signal from the satellite and to transform it into a compatible signal with a television set.

**ISO-7816**

This is the world standard for the CAM. The ISO term means "International Standards Organization" which is the world organization in charge of the development of these standards. Any apparatus indicating that it is in conformity with the ISO-7816 standard must be able to read/write on a CAM.

**IRD ID#**

Unique serial number written to the back of the receiver. This number is of the R00...type.
**JAVAEMU**

Name given to the computer emulation software written in Sun Microsystem's JAVA programming language.

**JTAG**

Represents "Joint TEAM Action Group". Consist of a plate located under certain receivers with soldered connections to the TSOP. It is used for reading or writing on the TSOP.

**KEY**

Public key being used to decrypt the satellite feed.

**LNBF** - Low Noise Block Converter with Integrated Feed

Amplifier which converts the microwave signal coming from the satellite into low frequency signals which are transmitted by a coaxial cable towards the receiver. A dish having two LNBF entries allows the connection of two receivers to the same antenna.

**Married**

Describes a CAM that can only be used with its receiver.

**MCG**

Association of programmers which provided us with the most powerful software for the programming of AVR boards and ROM2s and open ROM3s. The last version of software created from the work of MCG is **MCG308** which allows the programming of AVRs and solves the problem caused by the ECM of autumn 2001 on the Dishnetwork system. (BEV was not affected at this time).

**Nag Screen**

Nag screens are often caused by ECMs sent through the satellite feed to prevent piracy. Recently, an ECM nag screen informing you of a serious problem with the receiver along with a toll free number to call was being sent intermittently. Obviously this information was false and a trap in order for you to call the provider and thus denounce yourself.

**PPV - Pay Per View**

Channels with restricted access where the consumer must purchase a particular feature.

**Programmer**

Apparatus used to program a CAM emulator.

**Receiver**

Receiver of signals emitted by a satellite. The receiver has an integrated demodulator making it possible to receive a "rough" signal from the satellite and to transform it into a compatible signal which can be viewed on a television set.
**RAM**

"Random Access Memory", a type of inscribable storage unit. It's the type of memory used on a CAM to store information.

**Test Card**

Programmed and functional emulation board.

**TSOP**

Integrated circuit located inside the receiver. This circuit contains a unique number with each IRD (Boxkey) and is being used to generate the private part of the decryption process. On some receivers the TSOP can be accessed via a plate with soldered points of connection called JTAG. Actually, the term TSOP indicates the format of the integrated circuit.

**WINVU**

Name given to the computer emulation software running under Windows.

**Basic Notions:**

The satellite signals are emitted by a provider towards a satellite of transmission. These signals are encrypted (coded) to secure the provider's content. These signals are retransmitted by the satellite towards a designated zone. The satellite is geostationary in relation to the surface of the globe. The signals are retransmitted by the satellite towards its transmission zone. They are consequently collected by a subscriber's dish. The signals are reflected by the dish towards the amplifier (LNBF) which transforms these microwave signals into low frequency signals which are conveyed by the coaxial cable from the antenna towards the receiver.

The role of the receiver is to decipher (decode) these signals and to transform them into analog signals used by conventional television sets. For the decryption of the signal the receiver will need two keys. The first key is known as public because it is emitted with the signal coming from the satellite while the second key is known as private because it's generated by an algorithm which uses the Boxkey registered on a microprocessor called a TSOP and located in the receiver. So that the signal can finally lead to the television set, the receiver must validate the right of the consumer to receive the whole of the signal or only one part corresponding to the subscriber's purchased programming package. During the activation of the subscription by BEV, an command is conveyed from the satellite towards the receiver indicating to the receiver to register in its memory the data related to the subscription bought as well as the generation of the private key for decryption starting from the Boxkey of the IRD and the number of the CAM.

As soon as a CAM is programmed it is considered as being married to it's receiver. A CAM can only be used with the receiver to which it is married since the private decryption key is generated from the CAM and the receiver.

As long as the receiver makes this validation in a positive way, the signal is transmitted from the receiver towards the television set. We will now examine how it is possible to obtain every channel available by BEV without having to subscribe to the service.
STEPS TO FOLLOW TO OBTAIN THE ENTIRE PROGRAMMING:

- Determine if you wish to function with or without a subscription to BEV. To make this decision it is imperative to know that to function without a sub to BEV you must obtain your receiver’s boxkey. You must also determine the type of receiver you have because certain units do not have a JTAG port to read the TSOP. Here is a list of receivers with the annotation indicating the possibility, or not, of reading the boxkey using the JTAG. For receivers in which it is not possible to read the boxkey using the JTAG, you can also bring it to a dealer or technician who has the necessary equipment to read the boxkey directly from the TSOP. For models 3000, 3500, 4000 and 4500 it is possible to read the boxkey with a parallel port or using a standard voltmeter. To read via the parallel port download the Boxkey2 file at this URL:


then follow the instructions contained in the software. For the method using a voltmeter, download the file 3500.zip at:


and follow the instructions.

For the method using a voltmeter the credit is entirely due to baja... thank you infinitely for your assistance!

Boxkey accessible with a JTAG:

Models 2700, 2800, 3100(old), 3700, 3800, 3900, 4700, 4900, DP-301, PVR501, 5100, 6000, DRD420, DRD440 and DRD 480

Receivers without a JTAG:

Models 1000, 2000, 2200, 2500, 3000, 3100(new), 3500, 4000, 4500, 5000, 5500, DP7100, DP7200

NOTE: New model 3100 receivers do not have an opening to the JTAG connector. It is possible to access this by removing the receiver's main board. This will be explained further in the guide.

Further in this handbook you will learn how to build a JTAG and read your receiver’s boxkey. For the moment, let us determine if you can read your boxkey and if so, you can decide to function with or without a subscription. The advantages of knowing your boxkey makes it possible to use an AVR without having to insert the genuine CAM which can be required by some of the software for programming the AVR. As of writing this manual, EFA-Atmega boards require that you have the boxkey. For those who cannot read their receiver’s boxkey, you will have to follow the procedures by considering that you absolutely need to have or had a subscription with BEV to function.
• Build or buy an AVR or ATMEGA. An AVR or ATMEGA is an emulator which will make it possible to simulate the presence of the real CAM in the receiver. This board consists of printed circuitry on a fibreglass plate, of an ATMELE AT90S8515 microprocessor and a DB25 male connector and a ISO card reader. Atmega wafers consist of integrated micro circuitry on a thin plastic board with a crystal and Atmega microprocessor. These cards require an external programmer with a DB25 connector and ISO card reader.

If you wish to try and build your own AVR, the schematics and explanations are available at the following URL:


and the file to download is called: Tuckeravr305.zip.

If you wish to try and build your own Atmega, the schematics and explanations are available at the following URL:


You can also upgrade your current AVR by replacing the DIP format AT9028515 chip. Schematics and explanations are available at the following URL:


For an AVR or Atmega to function it needs various parameters (IRD#, CAM#, Type of board etc.) allowing it to emulate or replicate the operation of the true CAM as accurately as possible. This programming is stored on the ATMEL AT90S8515 or Atmega128 chip. The software used to program the data in the AT90S8515 uses all the storage capacity available in the circuit. When the first autoroll versions of these software were introduced (MCGAR101), one only had to program the AVR with pins 10 and 12 hooked together (11 and 14 on model PLCC) so that the AVR collects on it’s own the keys (AUX0 and AUX1) via the satellite signal and update itself according to the key changes. A command sent by BEV during the autumn of 2001 blocked the "autoroll" function. The programmers then put themselves to the task of solving the problem and provide users with a new software allowing to return to the autoroll mode. Programmers quickly realized that the software would occupy more memory capacity than what was available on the AT90S8515 circuit. The solution was to add a circuit to existing AVRs to increase the memory capacity available, and thus, to contain the new software. This autoroll mode was once again blocked in February 2002. To date, the additional circuit added on AVRs is no longer in use except for those having flashed their receiver TSOP with an earlier version of firmware or those using the more recent Turnip4.3 AVR software. For those who have this circuit on their boards it is not necessary to remove it, the current software allows programming of the AVR with this circuit in place. Before going on to the AVR programming part of this manual, it is wise to briefly explain the operation of all types of AT90S8515 circuit, 24LCxxx or 24Cxxx. So that these circuits can carry out the programming which they contain, they need an internal program indicating the operations to be carried out. This programming is called "Flash" and is the same one for all AVRs or Atmegas if it is made from the same software. Considering that certain parameters differ from one AVR to another (IRD#, CAM#, etc...), this data is then stored to the circuit in a particular memory called EEPROM. Thus in operation mode the circuit (for example the AT90S8515) carries out the basic program "the Flash", the basic program requires a value which can differ from one AVR or Atmega to another, the basic program will gather this information in the EEPROM section of the circuit. That is why all software for programming AVRs have commands making it possible to program, read or check the FLASH or the EEPROM of the circuit.
Programming the Flash and EEPROM of your AVR:

Let us proceed now to the programming of the FLASH and EEPROM of the AVR or Atmega. There are a multitude of software available to carry out this task. The most widespread is Jeepers. We will concentrate on the JeepersDX version 2.1.0 software since this version is the most complete to date.

- After having purchased or built your AVR or Atmega, it should now be programmed to make it functional. You recall that just like the genuine CAM provided with your receiver, a programmed AVR or Atmega will function only with the receiver for which it was programmed. For the programming, you must have access to a computer running under Windows 95,98, ME or XP with a DB25 parallel (printer) port and access to the Internet. You will also have to download the software available at this URL:


The file name is: **JeepersDX 2.1.0**

If you do not know your receiver's boxkey, only two possibilities are available:

1. Use a non autoroll enabled AVR and the Quincy1 software (used for AVRs without the 24LC256 chip or AVRs with the 24LC128 chip).

2. Use an autoroll AVR with the 24LC256 chip and Turnip4.3 software.

You are now ready to program your AVR. Launch the Jeepers software which you have downloaded and installed on your computer. The following window will appear:
PROCEDURE USING QUINCY1 SOFTWARE

In the Program field choose "Quincy's Fix"
In the Network field choose "ExpressVu"
In the Enabler Type field choose "Married Sub" since you intend to use your AVR with a valid smartcard and subscription.
In the Board field choose AVR3
In the IRD# field of the Receiver section enter your receiver's unique number written on the back of the unit. This number starts with R00...
In the CAM# field enter your smartcard's unique number written on the back. This number starts with S00...
In the keys section click on GET to obtain the 4 necessary public keys from http://keys.sattech.net

Here are a few more to add to your Jeepers "File", "Preferences" in order to GET the keys:
http://www.maxtek.net/keys.php/
http://www.charley.dynip.com/bev
http://www.evuavr3.com/keys/

PROCEDURE USING TURNIP4.3 SOFTWARE

From the top I2C choose Write AREEP200
In the Program field choose "Turnip4.3"
In the Network field choose "ExpressVu"
In the Enabler Type field choose "Married Sub" since you intend to use your AVR with a valid smartcard and subscription.
In the Board field choose AVR3
In the IRD# field of the Receiver section enter your receiver's unique number written on the back of the unit. This number starts with R00...
In the CAM# field enter your smartcard's unique number written on the back. This number starts with S00...
In the keys section click on GET to obtain the 4 necessary public keys from http://keys.sattech.net

Here are a few more to add to your Jeepers "File", "Preferences" in order to GET the keys:
http://www.maxtek.net/keys.php/
http://www.charley.dynip.com/bev
http://www.evuavr3.com/keys/

Whether you have programmed using Quincy1 or Turnip4.3, your AVR is now ready to be used in the receiver. However, protection measures on the receiver's TSOP & EEPROM are recommended. This will be explained further on. Insert your AVR in the receiver with the smartcard having been put in with the CAM# facing upwards.
Of the 4 public keys, those named Key0 and Key1 are not used by BEV but by the American networks. The Aux0 and Aux1 are those used by BEV. The satellite provider also sends these two public keys towards the receiver but only one is used by the receiver for decryption. Copy the value registered in Aux0 in the Public Key field of the CAM section. Then in the CAM section it is necessary for you to choose ExpressVu as type of network and to choose Key0 since it’s the Aux0 key which we programmed as the public key.

In the Time Zone section, you must choose the time zone corresponding to your location. For Eastern Canada this should be AST/EDT during the summer season (advanced Hour) and on EST/CDT autumn and winter (normal hour). In the Zip Code section just put “0” this field is used by the American systems and not BEV. Finally don’t change anything in the Password field and make sure that your AVR is connected to the parallel port of your PC. To be cautious, you should never connect the AVR while the PC is powered on. While manipulating your AVR, avoid static shocks which might damage your AVR’s circuitry.

The Min Tier and Max Tier fields must preserve the default values proposed by the software. For the Blackout field, click on the arrow at the right end of the field and choose the FF FF FF 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F value from the drop-down menu. You are now ready to program your AVR. By pressing on the Full Monty button of the software you will see the programming progress in the status bar. When it’s finished, turn off your computer then unplug the AVR from the parallel connector. Your board can now be used in your receiver. However, it is important to provide protections to your receiver to avoid any possible ECMs from the provider before using the AVR. To use insert your AVR in your receiver with the DB25 connector facing upwards, insert your CAM in your AVR with the microchip facing upwards. Receiver protection measures will be explored further on in this manual.

If your AVR does not function; program it again by changing the Public Key field of the CAM section of the software to the AUX1 key. Then in the CAM section it’s necessary for you to choose ExpressVu for network type and check Key1 since it is the Aux1 key which we have now reprogrammed as the public key. Do another Full Monty or Write EEPROM and voilà!

After having programmed your AVR, it will function as long as you don’t put your genuine CAM by itself in the receiver. We will take time here to explain the concept of public Key during the operation of the AVR with the genuine CAM. When the CAM is inserted in the AVR it is protected or shielded from the provider’s ability to write to it. This means that no information coming from the satellite signal can be registered on the microchip of the genuine CAM. For the AVR to work it must be able to communicate with the CAM and for this reason a communication code must be common to both cards. It’s important to understand this concept of common code which is completely different in terms from the use by the AVR of codes AUX0 and AUX1. Consider that a CAM is inserted in a receiver, it has then on its chip two codes present as the values of AUX0 and AUX1 sent by the satellite. Only one of these values is active, i.e. is used by the receiver for the decryption of the satellite signal. Let us suppose that the codes present on the CAM are:

AUX0: AA AA AA AA AA AA AA AA
AUX1: BB BB BB BB BB BB BB BB
The active key being AUX0
The value of AUX0 being in the Public Key field and checking the Key0 box to indicate that we use the value of AUX0 as the active key. At this time we are certain that the CAM and the AVR have the same common code of exchange, that is the value of AUX0. We then withdraw the CAM from the receiver and insert it in the AVR. From this moment on the CAM is protected and thus can't be written to by the provider. Now, what if BEV decides to modify the codes and transmits the following values via the satellite signal:

AUX0: CC CC CC CC CC CC CC CC
AUX1: BB BB BB BB BB BB BB BB
The active key being AUX1

Only the AVR will receive these new values and will register them in its memory if it is autoroll or you reprogrammed it with these new keys. In the case of the autoroll mode the AVR will not modify the values of the common code of exchange with the CAM which is registered on another part of its memory and which corresponds to the old value of AUX0 being : AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA. If you have changed the codes manually you don’t have to modify the code already registered in the CAM section in the Public key field. The AVR then uses the new keys received by the satellite signal to proceed with the decryption of the satellite feed and provide you with an image but will always use the same values of the common code of exchange with the CAM being : AA AA AA AA AA AA AA AA. Thus for those who understood this explanation, the update of the codes used by the AVR to provide you with a TV image does not change anything of the value of the common code of exchange.

As long as this common code is the same on the CAM and on the AVR you will be able to see an image. However, as soon as you insert your CAM by itself in the receiver, it will not be write protected anymore which means that new values will be registered on your CAM and these values will no longer correspond to the values which you programmed in the CAM section of your AVR using the Jeepers software. You will then have to reprogram your AVR to these new values.

- If you chose to function without a BEV subscription and you can read your receiver's boxkey you must retrieve this unique number before programming your AVR. It's important to specify that at the time this manual was drafted, it is impossible to function without a BEV subscription. To do this you will need to use the WinVu, CEMU or Javaemu software or a programmed ROM3 or Atmega card. These methods will be explained further on in this manual. To read your receiver's boxkey, you will need to build or buy a JTAG (named after the connector to which it connects on the receiver). You will find an illustration of a homemade JTAG at the following URL:

  http://www.geocities.com/electronics1ST/JTAG.html

- If you wish to build your own apparatus, a schematic and description are available at this URL:


and the file to be downloaded is named Very simple JTAG.zip

A more elaborate version with an integrated circuit is also available at this URL:

• You will also need a software to read this information from your receiver. This file is also available at this URL:

and the file name is Jkeys 2.0.0

To purchase a JTAG, simply visit our web site at http://www.maestra.ca and click the dealer banners. We recommend that you purchase items by COD only.

• After having built or purchased your JTAG, you can connect it to your receiver (powered-off) either by soldering if it’s a home made JTAG or by using the connector with a commercial JTAG. The JTAG connector is located under the receiver. We recommend that you consult the connection instructions provided with the Very simple JTAG.zip file for models x700 because it is well illustrated. For other models, here is a graphic illustrating the connection:

3100 MODEL (LSI SC2000 processor)

<table>
<thead>
<tr>
<th>DB25 Connector</th>
<th>100 ohms Resistor</th>
<th>Receiver JTAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin 2-----------/\-----------------------------------Pad3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 3-----------/\-----------------------------------Pad4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 4-----------/\-----------------------------------Pad5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 5-----------/\-----------------------------------Pad 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 13----------/\-----------------------------------Pad 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pins 18 to 25--------------------------------------------Ground</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

JTAG's pad numbers under a 3100 receiver

BACK OF THE RECEIVER – VIEW FROM UNDERNEATH

FRONT OF THE RECEIVER – VIEW FROM UNDERNEATH

5100 MODEL (STI55xx Processor)

<table>
<thead>
<tr>
<th>DB25 Connector</th>
<th>100 ohms Resistor</th>
<th>Receiver's JTAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin 2-----------/\-----------------------------------Pad 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 3-----------/\-----------------------------------Pad 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 4-----------/\-----------------------------------Pad 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 5-----------/\-----------------------------------Pad 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 13----------/\-----------------------------------Pad 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pins 18 to 25--------------------------------------------Ground</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
JTAG’s pad numbers under a 5100 receiver

**BACK OF THE RECEIVER – VIEW FROM UNDERNEATH**

<table>
<thead>
<tr>
<th>123456709</th>
</tr>
</thead>
<tbody>
<tr>
<td>666666</td>
</tr>
</tbody>
</table>

**FRONT OF THE RECEIVER – VIEW FROM UNDERNEATH**

6000 MODEL (STI55xx Processor)

<table>
<thead>
<tr>
<th>DB25 Connector</th>
<th>100 ohms Resistor</th>
<th>Receiver's JTAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin 2-----------////--------------------------------Pad 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 3-----------////--------------------------------Pad 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 4-----------////--------------------------------Pad 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 5-----------////--------------------------------Pad 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pin 13---------////--------------------------------Pad 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pins 18 to 25--Ground</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

JTAG’s pad numbers under a 6000 receiver

**BACK OF THE RECEIVER – VIEW FROM UNDERNEATH**

<table>
<thead>
<tr>
<th>123456709</th>
</tr>
</thead>
<tbody>
<tr>
<td>666666</td>
</tr>
</tbody>
</table>

**FRONT OF THE RECEIVER – VIEW FROM UNDERNEATH**

**ModchipMtl.com**

The REAL Atmega-EFA

80$ CAN & 55$ US
For new model 3100 receivers which do not have a JTAG access, here is a connection illustration:

Connect the DB25 connector of the JTAG to the parallel port of your computer. Obviously the computer and the receiver must be powered-off. Once connected, turn the computer on then turn on the receiver and load the JKeys software. Then you will see the following window:

If your JTAG connection is incorrect, this is the window you will see. If your connection has succeeded, you will see your receiver values registered before the "Device ID" and "Device" fields. These values may vary depending on the model of receiver you have. The software will register the number of the receiver in the IRD # field and will register the boxkey. If this data does not appear automatically you can press on the "Find Keys" button and if your connections are correct your boxkey will appear. It is possible to safeguard this information on floppy disks by pressing on the "Save Mem" button and by indicating a destination folder.
It should be noted that the software is conceived to read only the data relating to the number of the receiver and of the boxkey in an automatic way but it is also possible to read the entire data contained on the TSOP to save them as a safeguard in the event of failure or replacement of the TSOP.

For this you must know the (Start address) and the length of the data (Data Length or Byte). You will find this information in a document created by SatFTA and available at the following address:


Enter these values in the corresponding fields of the Jkeys software then press on the "Save Mem" button. This operation will be more or less long according to the type of receiver you have. A section on how to read/write to your TSOP will be covered in this manual.

**Computer Emulation Using WinVu:**

WinVu is an emulator which uses your PC connected to an AVR and receiver in order to decrypt the provider feed in autoroll mode. You will need a Pentium or AMD processor of at least 266 Mhz but some have reported successfully using a 166 Mhz. This information does not apply to Atmega boards.

**Equipment (minimum needed)**

- 1 DB9 connector (usually female) or DB25 depending on the type of serial port on your PC.
- 2-1Kohms ¼ watt resistors.
- 2 Zener diodes of 3.3V to 5.1V tension interval.
- Standard telephone cord or CAT5 cable (to connect receiver to PC)
- One AVR board with or w/out a DB25 connector.
- One 10uf 25 volt capacitor

The procedure consists in building a cable with a DB9 or DB25 (depending on PC serial port) connector on one end of the cable and a DB25 connector on the other. Two schematics will be presented according to the type of PC serial port connection you require. It is important to note the resistor and diode positioning as well as the diode black stripes orientation.
Connecting to the PC DB25 serial port:

In certain cases, the resistors will have to be replaced by 820 ohms if you are unable to run WinVu (particularly when using laptop PCs)

It is also possible to connect the cable directly to the Atmel chip of your AVR if it is not equipped with a DB25 connector. The following schematic can be used:

Software Section

You are now ready to program your AVR to communicate with the PC. For this, you will need to download Ird2pcj.zip at:  

Extract and place ird2pc.pfg and ird2pcv2.pfg in the same program folder as the Jeepers software.
Next, create a folder named WinVu and download the WinVu2008 software at:


Extract the contents of WinVu to your folder and browse to it in order to locate a file named Mscomm.ocx. Copy this file in your C:\Windows\System directory. You will also need to search your computer for the following file: MSVBVM60.dll. If you do not have this file, you can download it from:


Simply install this in your C:\Windows\System folder.

If you are running under Windows 2000/XP you will have to copy the Mscomm.ocx file in the C:\Winnt\System32 or C:\Windows\System32 folder.

You will then have to register this in the Windows Registry. Click on Start then Run. At the command prompt type regsvr32 mscomm32.ocx and hit Enter.

If your AVR is of the “wafer” type and you wish to emulate using WinVu, here is a table describing direct connections to the Atmel chip:

```
PLCC type Atmel

Pin 7 of the Atmel connected to pin 9 of the DB9 connector
Pin 9 of the Atmel connected to pin 2 of the DB9 connector
Pin 22 of the Atmel connected to pin 5 of the DB9 connector
```
TQFP type Atmel

Pin 1 of the Atmel connected to pin 3 of the DB9 connector
Pin 3 of the Atmel connected to pin 2 of the DB9 connector
Pin 16 of the Atmel connected to pin 5 of the DB9 connector
Programming and startup

You are now ready to program your AVR. Plug your board to the PC's parallel port and start the Jeepers software. In "Program" choose "Lotec308". Insert your IRD, CAM and boxkey numbers in the appropriate fields. Go back to "Program" and change it to "ird2pc" if your AVR’s pin 10 and 12 are not jumpered. If so, choose "ird2pcv2" instead. Click on "Full Monty" and your AVR will be programmed. Close Jeepers and unplug your AVR from the PC.

The next step consists in converting your receivers ID and CAM numbers to hexadecimal format. WinVu will need this conversion in order to work.

Start your Windows calculator and convert it to scientific mode and check the DEC field. Enter your receiver's ID number and check the HEX field. If this value does not contain 8 numbers, add 0s to the beginning in order to obtain a value of 8. Save the converted value for later use. Repeat this conversion for your CAM number.

Go to your WinVu folder and start WINVU2008.exe

Insert the converted hexadecimal IRD and CAM numbers you had saved in the appropriate fields. It is important to insert any letters in CAPS only.
In ZP field enter a ZIP code, only the American codes are valid thus choose a ZIP code of an American city in the same time zone as you. Ex: Quebec the value of 03103 corresponds well.

In the Tz field choose the time zone corresponding to your zone. For Quebec the value of EST is in conformity when we are in standard time and AST is in conformity when we are in daylight savings time. In SID field keep the default value. Choose the port corresponding to the one active on your computer (usually COM1 or COM2) then choose 115,200 for the speed of the port.

Select Rev380 in the Rev field so you don’t get the 104 nag.
Choose High in the CPU field to run WinVu in priority on your computer.

Check Autoroll, Ird2pc and Display then click on the Apply button.

The configuration of WinVu is now finished. Let’s now jump to the configuration of your PC’s serial port. On your computer click on the Start button then choose Parameters and finally Control panel. In the control panel click on the System icon to open it. Now select the peripherals manager then in the list click on the + sign in front of Ports (COM and LPT). You should have a window similar to this one but in English:
Click now on the Properties button at the bottom of the window and choose the Parameters of
the port. You should now have this window on the screen:
Insert the following values:

- Baud Rate: 115200
- Parity: None
- Data Bits: 8
- Stop Bits: 1
- Flow Control: No Flow

Click OK to come back to your desktop and shut down your computer.

Unplug your receiver for at least one minute. Connect the cable to the AVR and the computer and insert AVR in receiver. Start both computer and receiver then start the WinVu software by clicking WinVu.exe in your WinVu folder. In WinVu click the START button. The FW-BS fields should automatically update themselves as well as the KEY0 and KEY1 fields. After approximately one minute the Authorization light should turn green. Here is what you should see on screen:

![WinVu software interface](image)

For the IRD-CAM, FW-BS and boxkey you should have your own numbers, this is just an example.

You can uncheck the Display field in order to save system resources. You can also download winvttool.zip. This utility will allow you to minimize the WinVu window to your system tray, a nice addition to the software.
WinVu Troubleshooting

The Smart Card Not Inserted Correctly error message is caused by WinVu not being able to communicate with the receiver. The most likely causes are:

1. Inappropriate serial cable.
   • Verify your cable for bad connections or short circuits.

2. AVR is not programmed correctly.
   • Reprogram your AVR as instructed making sure all appropriate values are inserted correctly.

3. Invalid or deactivated serial port.
   • If your PC has two serial ports, try connecting to the other available port. You may also have entered the wrong port to use, try setting a different port. WinVu can remain in operation while you change this value.

4. COM port conflicts.
   • If your PC has an internal modem, check the settings to make sure it doesn't use the same system resources as your COM port. Also make sure your COM ports are all activated in your BIOS settings.

5. No capacitor
   • If you haven't installed the capacitor as mentioned, please do so now.

6. Resistor values
   • Try lowering the resistor values from 1K to 820 ohms

7. Serial Port Communication Problem
   • To verify if there is serial port communication, you can do an echo test. To do this, connect pins 2 and 3 DB9 WinVu cable and connect it to the computer. Start HyperTerminal (installed with Windows) and configure a connection on the port you are using as illustrated below:
From the first window click OK and the second "Connect" window will appear.

Type a text in the Hyperterminal window and it should appear. If the text does not appear, you may have serial port communication problem. This test can also be done to verify the WinVu cable itself. Instead of connecting pins 2 and 3 of the DB9, do this same procedure for the DB25 connector. This will only work if you have chosen the correct serial port number.

**COMPUTER EMULATION USING JAVAEMU:**

JavaEmu is an emulator which uses your PC connected to an AVR and receiver in order to decrypt the provider feed in autoroll mode. You will need a Pentium or AMD processor of at least 266 Mhz but some have reported successfully using a 166 Mhz.

Steps to follow:

1. Create a communication cable as explained in the WinVu section of this manual.

2. Download and install the **Java Runtime 1.4.0** file from:

3. Download and extract to a folder the **Java Comm Api v2.0** files from:

4. Download the **Javaemu0.4.3** file available at:

5. Download and extract to a folder **Codegen102** available at:

6. Download **vu-dump.bin** available at:

7. Download **xCel3.0** available at:

8. Install the **Java Runtime 1.4.0** by following the on screen instructions. Use the default folder destination.

9. From the folder containing the **Java Comm Api v2.0** files, copy the following files to their appropriate folders:
   - Win32com.dll to `C:\Program Files\Java\j2re1.4.0\bin`
   - Javax.comm.properties to `C:\Program Files\Java\j2re1.4.0\lib`
   - Comm.jar to `C:\Program Files\Java\j2re1.4.0\lib\ext`

   After copying these files, double-check to make sure they are in the correct folders.

10. From the previously downloaded **Javaemu0.4.3** file, extract **Javaemu043.jar** and **rom3.bin** to your `C:\Program Files\Java\j2re1.4.0\lib` folder.
11. Create a JavaEmu batch file by copying the following code in Notepad and saving it as java.bat

c:
cd\ncd progra~1
cd Java
cd j2re14~1.0
cd lib
java –cp JavaEmu043.jar MainForm

12. The next step consists in making a Rom3 image which JavaEmu will use. Start the xCel software and choose "Open bin" from the "File" menu. Browse to \vu-dump.bin file you have previously downloaded.

13. As instructed in the WinVu section of this manual, convert your IRD and CAM numbers to hexadecimal format and enter them in the appropriate fields. Next, enter the same American Zip Code as in WinVu. The KEY0 and KEY1 fields must be the valid AUX0 and AUX1 values at the time of programming. Insert your boxkey and Time Zone values (ie. Eastern-F0 for Eastern Standard Time) and 85 for the PPV amt. The Blackout value should be 00 00 B4 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F 7F.

14. From the "File" menu choose "Save card info" name and save it to a location.

15. While xCel is running, start Codegen102. Select the Rom3, 3M Activation and ExpressVu fields as indicated below:

![Codegen102 screenshot](image-url)
16. Click on the "Generate Code" button. A codegen.ne3 file will be created and you can now close **Codegen102**.

17. Go back to xCel and from the "EEPROM Utilities" menu choose "Patch EEPROM" and browse to your codegen.ne3 file and click on "Apply the changes to the currently open eeprom".

18. Your image has been created.

19. From the "File" menu choose "Save bin as" and save it to **C:\Program Files\Java\j2re1.4.0\lib**

20. Program your AVR using Jeepers and ird2pc or ird2pcv2 as instructed in the WinVu section of this manual.

**JavaEmu StartUp**

1. Insert the AVR in your receiver and connect the communication cable from the PC to the AVR.

2. Plug your receiver to the outlet and power up. Start the JavaEmu software by clicking the Java.bat file you previously created. If you have followed the instructions correctly, this is the window that should appear:
3. Choose your COM port and click the "Start" button. If everything is functioning correctly, the "start time", "start date", "current time" and "current date" should update themselves.

4. Your software will convert to autoroll once the card image changes from Rev372 to Rev380 by the satellite feed. The time this takes varies.
COMPUTER EMULATION USING CEMU:

CEMU is an emulator which uses your PC connected to an AVR and receiver in order to decrypt the provider feed in autoroll mode. Very similar to WinVu and JavaEmu but uses much less system ressources since in runs in DOS mode.

Here is the procedure to follow:

1. Download and extract the contents of Easy_cemu_emulation.zip which can be downloaded from: http://www.maestra.ca/english/files/index.php?action=file&id=7

2. Make or purchase a cable as mentioned in the WinVu section of this manual.

3. Program your AVR as mentioned in WinVu.

4. We will now modify the Cemu.ini file. This file should be found in the program folder in which you have installed the CEMU software.

5. Open the cemu.ini file in a text editor and modify the values corresponding to your IRD and boxkey numbers, the port you are using (Com1 or other) and the time zone you are in. Here is the contents of the file with the zones to modify in red:

```
# For comments any option use the symbol #
#
# Port is 1 for COM1, 2 for COM2 , 3 for COM3 .....#
#
port=1
# Baud Rate Available 9600,14400,19200,38400,56000,57600,115200
baud=115200
#
# Ajust the FIFO for serial port
# RX FIFO Buffer 1,4,8, 14
#RXThreshold=1
#
# TX FIFO Buffer 1 to 16
#TXTThreshold=1
#
# Disable FIFO = 1 or Enable = 0
#FifoDisable=0
#
# If your commport don't use the sandard IRQ and Base Address.
# Change the following parameter IRQ and BaseAddress
# Standard IRQ and BASE Address.
```

We Are The First Authorized Official Atmega-EFA Retailer
# Port  Base Address  IRQ
# COM1   0x3f8       4
# COM2   0x2f8       3
# COM3   0x3e8       4
# COM4   0x2e8       3
#
# IRQ Number for your COMM Port
#IRQ=4
#
# I/O Base Address
#BaseAddress=0x3F8
#
# The name of your ROM file
rombin=rom3.bin
#
# The name of your EEPROM file (Choose)
dishbin=Bev380.bin
#
# Enter your parameter For ROM3 rev A in this file or use XCel and comment the line with #
# All value in HEX same of WinVu
#
# BoxKey (ADDRESS 0xE421)
boxkey=0000000000000000
#
# CamId (ADDRESS 0xE038)
# CamId (ADDRESS 0xE42F)
# CamId (ADDRESS 0xE4E4) REV A
# CamId (ADDRESS 0xE4EB) REV B
CamId=01234567
#
# IrdNum (ADDRESS 0xE40D)
IrdNum=00000000
#
# BlackOut (ADDRESS 0xE4FC)
BlackOut=0000B4FFFFFFB4B4B4B4B4B4B4B4B4
#
# Choose the Daylight Saving
# For Daylight = 1
# No Daylight = 0
Daylight=1 (For daylight saving choose 1)
#
# Choose a good Time Zone work with Zip Code and DayLight (ADDRESS 0xE40B)
#
# ALASKA
# EASTERN
# CENTRAL
# MOUNTAIN
# PACIFIC
# ATLANTIC
# NEWFOUNLAND
# VIRGIN
# HONOLULU
TZ=EASTERN (Choose a good Time Zone work with Zip Code and DayLight)
3. Start your computer and after a few seconds you should see a series of numbers appear on screen and an image on your television.
OPEN ROM3 SMARTCARDS:

Older model receivers were shipped with Rom3 type smartcards. These cards had a defect which enabled satellite testers to reprogram the chip with the desired programming package or all channels.

In February of 2001, satellite providers launched a first ECM (Electronic Counter Measure) to close the door on these cards. Methods to circumvent this ECM were quickly adapted by the testing community and once again these cards were opened. In July 2001 a second ECM was introduced which once again closed the door on Rom3 smartcards. Very recently, American Dish Network cards were reopened for programming but the Canadian ExpressVu Rom3s remain closed and are currently being studied by various online communities (search for Project EMM). More recently the Dish Network testers found a way to reopen these cards and two weeks ago this was also discovered for BEV revision 372, 375 or 378 cards.

To this day, there are still open Rom3 cards available on the market. These cards have either been kept out of the provider streams or have been reprogrammed with blocker code to prevent them from being closed. For those fortunate enough to have one of these cards, the following section describes how to reprogram them:

Equipment

An ISO-7816 compatible programmer with a 3.6864Mhz crystal.
Open Rom3 BEV or DISH smartcard.
DB9 to DB9 "Straight Through" cable.

Software

Download and install Nagraedit2.0 available at:

Download and extract to a folder May3mfix.zip available at:

NagraEdit HowTo:

1. Please note that Nagraedit will only operate on a PC of 166Mhz or higher. For slower PCs, download and use FreeTalk instead.

2. Connect the programmer to a power outlet and a PC using the DB9 cable. Start the computer and launch Nagraedit, the following window will appear:
3. Click on the various menus in order to familiarize yourself with the software. Click on the "Tools" menu and choose "Options" to make sure that the appropriate COM port is selected and crystal setting is set to 3.6864Mhz. Insert your Rom3 card in the 7816 reader. From the "Card" menu choose "Read from card" or the menu icon with a blue arrow pointing towards the left. A message will appear in the text window. If you are trying to read a "Locked" CAM, the following error message will appear:

Opening of COM1 was successful
Logging into card
Card ATR is invalid
Error reading image from card
If you are trying to read a Rom10 type card, the following message will appear:

```
Opening of COM1 was successful
Logging into card
ROM Revision : 011
EEPROM Revision: RevB82
Error, this program only works with ROM2 & ROM3 cards
Error reading image from card
```

When reading a Rom2 card, the following message will appear:

```
Opening of COM1 was successful
Logging into card
ROM Revision : 002
EEPROM Revision: Rev052
Checking for back door
Backdoor appears to be open, continuing...
Retrieving ROM2 backdoor password
PASS WORD: 2F
Login successful
Reading image from card
Card read successfully with 1 retries
```
4. Click on the "EEPROM Data" tab and the following window will appear:

As you can see, this window contains vital CAM information fields and can also be used to edit these.

5. Next, click on the "EEPROM Editor" tab to display the following window:
Important Rom2 information are contained at the following lines of code:

$\$E000$ : Unique CAM information corresponding to the CAM number.
$\$E007$ : The "MAP" function. If a value of FF is indicated, this means your card has been marked by a reopening or an ECM. This card will be reusable only under certain conditions such as the use of a program to mask this mark.
$\$E010$-$\$E01F$ : The buffer stack. This zone can be programmed once and remains unaffected.
$\$E038$-$\$E03B$ : CAM identification zone #1
$\$E9A$-$\$E9E$ : Zip Code / Time Zone
$\$E940$ : Inverted hexadecimal receiver number
$\$E953$-$\$E95A$ : Boxkey
$\$EA3D$-$\$EA44$ : Key0
$\$EA45$-$\$EA4C$ : Key1
$\$EACB$ : Receiver Byte Status (Byte status 80=suspended, 00=normal)
ROM3 CARD

There are two Rom3 type cards, revision A and B. To find your card's revision, rom the "Card" menu choose "Read from card". Click the "EEPROM Editor" tab and scroll down to line $E4D0. Under columns "E" and "F", if a value of 07 38 is indicated, you have a Rev.A type card. A value of 07 05 indicates a Rev.B type card.

Here is a ROM3 Rev.A type card:
Here is what a ROM3 Rev.B type card looks like:

Upon reading with the programmer, a Rom3 Rev. A or B will display the following:
After successfully reading your smartcard, you will want to save the values for future use. From the "File" menu choose "Save card image". You will now choose a name and folder for your file. The software will assign a *.bn2 or *.bn3 file extension according to your card's revision type.

Click on the "EEPROM Editor" tab. As per the Rom2 card, this window contains Rom3 vital information which can also be edited.

Continue by clicking the "EEPROM Data" tab. Again, this window contains your card's information but in hexadecimal format. You can modify your card's values as needed. **WARNING: NEVER EDIT VALUES BETWEEN LINES $E000 AND $E02F. THIS ZONE CAN ONLY BE PROGRAMMED ONCE AND REMAINS UNAFFECTED.**

Important Rom3 Rev.A information are contained at the following lines of code:

- **$E000**: Unique CAM information corresponding to the CAM number.
- **$E007**: The "MAP" function. If a value of FF is indicated, this means your card has been marked by a reopening or an ECM. This card will be reusable only under certain conditions such as the use of a program to mask this mark.
- **$E010-$E01F**: The buffer stack. This zone can be programmed once and remains unaffected.
- **$E038-$E03B**: CAM identification zone #1
- **$E047-$E04A**: Zip code
- **$E04B-$E04C**: Time zone
- **$E04D-$E050**: Inverted hexadecimal receiver number
- **$E04D-$E04E**: Boxkey
- **$E04E-$E04F**: CAM identification zone #2
- **$E04F-$E050**: CAM identification zone #3 (Rev. A only)
- **$E050-$E051**: Key0
- **$E051-$E052**: Key1 for Rev. A only
- **$E059**: Receiver Byte Status (Byte status 80=suspended, 00=normal)

Important Rom3 Rev.B information are contained at the following lines of code:

- **$E000**: Unique CAM information corresponding to the CAM number.
- **$E007**: The "MAP" function. If a value of FF is indicated, this means your card has been marked by a reopening or an ECM. This card will be reusable only under certain conditions such as the use of a program to mask this mark.
- **$E010-$E01F**: The buffer stack. This zone can only be programmed once and remains unaffected.
- **$E038-$E03B**: CAM identification zone #1
- **$E047-$E04A**: Zip code
- **$E04B-$E04C**: Time zone
- **$E04D-$E04E**: Inverted hexadecimal receiver number
- **$E04D-$E04E**: Boxkey
- **$E04E-$E04F**: CAM identification zone #2
- **$E04F-$E050**: CAM identification zone #3 (Rev. A only)
- **$E050-$E051**: Key0
- **$E051-$E052**: Key1
- **$E059**: Receiver Byte Status (Byte status 80=suspended, 00=normal)
Programming With NagraEdit:

1. Before you start editing your Rom3 card it is very important that you save the current information for future use. Insert your card in the programmer and from the "Card" menu choose "Read from card". Then, from the "File" menu choose "Save card image". Insert a file name and save to both your hard drive and a floppy disk.

2. To successfully program your card, you will need to apply the files contained in May3mfix.zip in the following order. From the file menu choose "Apply a patch file" and browse to the folder where you extracted the files and choose Bev1.ne3
WARNING: THE FOLLOWING INFORMATION IS TO BE USED ONLY AND ONLY IF YOUR CARD IS NOT MARKED AT $007 - IF SO, GO TO STEP 7

3. Repeat step 2 for files Bev2.ne3 and Bev3.ne3.

4. From the "Card" menu choose "Write to card"

5. Click the "PATCH Editor" tab and click the "Run Patch" button. If you have followed the previous instructions correctly, the following information will be displayed:

![PATCH Editor Interface]

Patch applied with 0 errors and 0 warnings.
6. Your card is now ready to be used with the receiver. Repeat step 1 to save the card information under a new name.

7. If your card is marked at $007, follow these instructions. Note that if your card is marked, you will only be able to use it in non autoroll mode meaning that the card will have to be reprogrammed following each provider key change.


Start xCel3.0 and from the "File" menu choose "Open Bin" and browse to the vu-dump.bin file you previously downloaded.

From the "Tools" menu choose "Patch EEPROM" and browse to the location where you have extracted the contents of May3mfix.zip and choose **Bev1.ne3**, **Bev2.ne3**, and **Bev3.ne3** files.

From the "EEProm Utilities" menu choose "007Fix"

Enter your CAM and IRD numbers in hexadecimal format. Enter your Boxkey, your time zone (Eastern F0) and finally the AUX0 and AUX1 in the Key0 and Key1 locations.

From the "Card" menu choose "Write Current EEPROM" and "Write Full EEP excluding OTP". The card can now be used with your receiver. The following page contains an illustration of the xCel GUI to help you understand the previous instructions.
HOW TO OPEN A REV 372, 375 OR 378 ROM3 CARD

1. Download the file Na_worm_Bev from the following address: http://www.maestra.ca/english/files/index.php?action=file&id=24

2. From the zip file extract na_worm_bev.pfg into your Jeepers program folder.

3. Connect an LED diode between pins 20 and 24 of the Atmel AT90S8515 on your AVR. Connect the diode positive (+) to pin 24.

4. Program your AVR with Jeepers having chosen NA_WORM_BEV as the program and click FULL MONTY

5. Insert your ROM3 card inside the ISO slot of the AVR and insert the AVR in an ISO programmer with a 3.6864 Mhz crystal

6. Wait until the LED turns off, this should take between 10 seconds to 10 minutes. After this procedure, your card should be in an open state. Note that this will not work for REV 380 cards or marked (looped) cards.
HOW TO CHANGE THE TSOP Firmware

1. First off, a friendly warning; The following procedure could render your receiver inoperable if it is not done correctly and is not implied for inexperienced testers. If in doubt, ask an experienced person to do this for you.

2. If your receiver model is a 2700 or 3700, download the file patch.zip and extract its contents to a folder. File can be found at:

3. If your receiver model is a 4700, download the file patch.zip and extract its contents to a folder. File can be found at:

4. If your receiver is a 3100, download the file 3100-10UNE335.zip and extract its contents to a folder. File can be found at:

5. Again, for a model 3100, download the file hw32v25.exe and extract its contents to a folder. File can be found at:

6. Proceed to do a complete READ of your TSOP as explained in the "READ/WRITE to the TSOP using a JTAG" section of this manual.

7. Save this original TSOP data to a file, floppy disk or both.

8. If your model receiver is a 2700 or 3700, extract the contents of the appropriate patch.zip file which you have downloaded. Start patch.exe and from the "File" menu choose "Open" and browse to the folder where you have saved a "COPY" of your original TSOP data. Warning, this procedure will modify the data, please make sure you are using a copy of the original TSOP data and have a backup saved in case this fails. Upon opening the file, the application will indicate that it has modified the data. It is this modified data that will be used to reflash your TSOP further on.

9. If your model receiver is a 4700, extract the contents of the 4700patch.zip file which you have downloaded. Start 4700E223patch.exe and from the "File" menu choose "Open" and browse to the folder where you have saved a "COPY" of your original TSOP data. Warning, this procedure will modify the data, please make sure you are using a copy of the original TSOP data and have a backup saved in case this fails. Upon opening the file, the application will indicate that it has modified the data. It is this modified data that will be used to reflash your TSOP further on.

10. If your receiver is a model 3100 with two TSOPs named here IC23 and IC22. After having read both TSOPs as indicated in the "How to go from Bell ExpressVu to Dish Network" section of this manual, you will have to make a copy of these files to be modified and rewritten to your TSOPs. Open the HexWorkShop editor and from the "File" menu choose "Open". Browse to and open the TSOP IC23 copy. Copy lines 0000FFC0 to 0000FFF0. Now open the E335-EAEA-1FC00000-nonag.bin file which you have downloaded at the beginning of this tutorial and copy these lines (0000FFC0 to 0000FFF0). From the file menu choose "Save". The IC22 does not need to be modified.
11. All you have to do now is to reprogram your TSOP as explained in the "READ/WRITE to the TSOP using a JTAG" section of this manual.

12. After having reprogrammed your TSOP, you should only program your AVR as mentioned in this manual.
HOW TO GO FROM BELL EXPRESSVU TO DISH NETWORK:

People have asked me questions concerning ways to receive the American Dish Network feed using Bell ExpressVu model receivers. Before we delve into this procedure, it is important to note a few facts. In many cases, receivers used by BEV & Dish are the same (2700, 3100, 3700, 4700, 5100) but with one particularity, they can only download the provider firmware once for each provider. In other words, a receiver with BEV firmware downloaded to it can be pointed towards Dish Network and download the firmware but can't come back to BEV and redownload the firmware simply by pointing the dish to the provider's satellite. In such a case, the receiver's TSOP will have to be reflashed with the BEV firmware so you have now been warned. There must also be compatibility between provider receivers. For example, a Dish Network model 3800 receiver does not exist on the BEV provider and thus can't be used.

1. Buy or build a Jtag cable to read your receiver's boxkey. Instructions on how to build this are included at the beginning of this manual. You will now have to read your TSOP not only for the boxkey but for the entire TSOP. To do this you will need the JKeys software and follow the previous instructions except for the starting address and byte length to be inserted in JKeys. You will have to click the "Save Mem" button to save your entire TSOP information. Note that models 3100 and 5100 are equipped with two TSOPs and must both be read and saved. Here is a table showing values for different model receivers:

<table>
<thead>
<tr>
<th>MODEL</th>
<th>START ADDRESS</th>
<th>BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>2700</td>
<td>7FF80000</td>
<td>80000</td>
</tr>
<tr>
<td>3700</td>
<td>7FF80000</td>
<td>80000</td>
</tr>
<tr>
<td>4700</td>
<td>7FE00000</td>
<td>200000</td>
</tr>
<tr>
<td>3100 ic23</td>
<td>1FC00000</td>
<td>200000</td>
</tr>
<tr>
<td>3100 ic22</td>
<td>FDE00000</td>
<td>200000</td>
</tr>
<tr>
<td>5100 ic U7</td>
<td>7FC00000</td>
<td>400000</td>
</tr>
<tr>
<td>5100 ic U6</td>
<td>7F800000</td>
<td>400000</td>
</tr>
<tr>
<td>6000</td>
<td>7FC00000</td>
<td>200000</td>
</tr>
<tr>
<td>6000</td>
<td>7FE00000</td>
<td>200000</td>
</tr>
</tbody>
</table>


3. If both TSOP dumps are identical, you can continue on to the next step. Download and copy the MCG308 file in your Jeepers program folder.

4. Connect your AVR or Atmega to the computer and program using the following parameters:

FOR AN AVR BOARD

In the **Program** field choose **MCG308**
In the **Network** field choose **Dish**
In the **Enabler Type** field choose **Married Sub** (if this is the case)
In the **Board** field choose **AVR3**
In the **IRD#** field enter your receiver number starting with **R** (on back of receiver or from the sys info screen)
In the **CAM ID** field enter your smartcard number starting with **S** (on back of smartcard or from the sys info screen)
In the **KEY** fields, click on **GET** and Jeepers will connect to the address configured in the "File" "Preferences" section of the software. The keys on our web site can be found at:

http://www.maestra.ca/keys

Of the 4 keys, only Key0 and Key1 will be used. AUX0 and AUX1 are only used by BEV and not Dish. In the provider feed, these keys are sent to your receiver but only one is used to decrypt the signal and this is the key that will be placed in the **Public Key** field so copy **Key0** here and check **Key0** below.

In the **Time Zone** field choose your appropriate time zone (EST/ADT for Eastern Standard Time)
In the **Zip Code** field enter the American value of **03103**

Finally, do not enter any value in the password field. Connect your AVR to the PC parallel port. To be cautious, you should never connect the AVR while the PC is powered on. While manipulating your AVR, avoid static shocks which might damage your AVR’s circuitry.

Click "Full Monty" to program the AVR. You will notice the status bar indicating the programming in progress. Once done, shut down your PC and unplug the AVR. Note that once your AVR in the receiver, if you only get a black screen with the channel guide available, this means that the public key you have chosen is wrong. Repeat step 4 by copying Key1 in Public Key and check Key1 below.

5. Now that your AVR has been configured for Dish Network, you are ready to point your dish towards satellite 119. You can find the exact coordinates using this utility:


Note that Dish Network satellites are called EchoStar. Do not forget to do the Geographic and Magnetic North correction as indicated on the site.

6. Power on your receiver and from the remote control press the "Menu" button, choose "System Setup" and then "Installation". From the "Installation" menu choose "Point Dish/Signal" and try to obtain the highest signal strength value while pointing towards Dish Network's satellite 119.

7. Upon a high signal strength, power off your receiver and insert your smartcard. If your TSOP and EEPROM are locked, you will need to release them for the Dish Network update to occur. Power on the receiver and go to channel 101 and power off again for one hour. Afterwards, power up and you should have the Dish Network guide by pressing the remote control "Guide" button. Note that you will still be without programming at this moment.

8. Remove your smartcard from receiver and insert in the ISO slot of your AVR and put both in receiver and power up.

9. After a few minutes you should have all Dish Network programming available.

10. Do two more TSOP dumps and compare them to save for future use.

11. In order for Dish Network to function, your TSOP must be unlocked otherwise you will constantly get an error nag. If you are concerned by the fact your TSOP is unlocked, you can always use a lock discussed in "Protection Measures - Locks" of this manual.
FOR AN ATMega BOARD

Place the jumper on your card.
In the Program field choose “NawapoM0.0”.
In the Board field choose Atmega128 @18.0000Mhz.
In the Receiver section enter your IRD# (starts with R00...) and CAM# number (starts with S00...).
In the BoxKey field enter your boxkey number.
In the Key fields, leave the values at 00 00 00 00 00 00 00 00.
Enter your appropriate time zone in the field for this.

PROTECTION MEASURES – LOCKS:

Satellite service providers know about piracy and constantly try to stop it. To do this they introduce ECMs or electronic counter measures in the data stream. A counter measure can be as simple as a minor encryption key change or major such as firmware update which tries to render AVRs obsolete. Counter measures are not fully understood and thus should not be ignored. The objective is to lock out these ECMs with two known methods. The first is to lock the receiver's EEPROM and also the TSOP.

This locking method consists in denying the provider access to these chips. This protection should be done by a technician as it involves precise soldering on the receiver's main board. If you still would like to try and do this yourself, schematics are available at the following URLs:

Models 2700,3000,3500, 3700,4000,4500,4700

Models 3100 and 5100
using the 2700 schematic.
Involves unlocking every time the CAM is removed from the receiver or receiver is turned off.
and download the 3100.zip file. This file shows how to automatically lock the TSOP.

At the time this manual was created, TSOP locks for model 6000 receivers are still unavailable and model 5100 is being investigated. However, the 5100 model's EEPROM can be locked using the same method as the 3100 or 2700 models even if the EEPROM is a 24LC64 type. There has been a rumor on discussion forums that locking model 3100's EEPROM causes picture freezing. This has been proven to be false if the same method is applied as the 2700 model. Model 1000 EEPROM can only be locked if the chip is an Atmel 24C08A type otherwise the 24C08 can not be locked.

If you would like to test your locks when done, the EEPROM lock is relatively easy to test. Simply power on your receiver and modify your language setting in BEV's menu and save this modification. Power off the receiver and unplug for 30 seconds. Power on and if your language modification has not been saved, the lock has been successful.

It is now obvious that if you wish to make any other changes to your menu configuration you will have to unlock the EEPROM. You should always power off the receiver before changing from locked to unlocked mode.
To verify that the TSOP lock was successful is a little more complicated. This involves pointing your dish to another provider that BEV to see if the firmware will be updated. We won't go into further detail of this operation but you can find more information on this by visiting online discussion boards such as http://www.sattech.net or http://www.id-discussions.com. If you have followed the instructions, your TSOP should be locked as well.

**RECEIVER & TELEPHONE LINE:**

When legally using BEV's services and purchasing a PPV feature, this information is written to your smartcard's microchip. The memory on this chip being limited to about 10 purchases, the receiver is equipped with a modem which dials in to BEV's billing center. There is no other reason for this feature except maybe to verify that you are using a device to pirate their services. That being said, whether you are testing this provider with or w/out a legal subscription, **NEVER PLUG THE PHONE LINE TO YOUR RECEIVER!**

**DOWNGRADING YOUR SUBSCRIPTION:**

If you've just joined the AVR satellite testing community, you will no doubt want to downgrade your subscription. To do this, simply call BEV's customer service number and ask for the package that suits your budget, there is absolutely nothing wrong with doing this while your AVR is in the receiver. The customer service representative will ask you for your CAM ID and revision number. **Simply answer that you are not at home or in front of your receiver to give them this information.** The representative will accept and validate your new subscription. If you wish to do this the regular way, remove your AVR and insert your CAM in the receiver, plug the telephone line and remove your locks before calling. Again if you choose this method, **remove your AVR from the receiver** because if you don't, you will be giving the AVR's revision number and not your smartcard's number from the sys info screen to the BEV representative and will surely be in trouble.
MISCELLANEOUS INFORMATION & TROUBLESHOOTING:

Receiver Master Reset

To do a receiver master reset, follow these steps:
With the remote control press Menu
Choose System Setup
Choose Diagnostics
On the remote press the Info button
Press the Right Arrow button
Press the Left Arrow button
Press the TV/VIDEO button
Press the Select button
Unplug your receiver for 30 seconds.

Your receiver should now be reset to the original configuration with parental locks removed.
Note that this does not remove any PPV purchases from your CAM.

For model 5100, a different Master Reset procedure is required:

With the remote control press Menu
Press the number 6 button
Press the number 3 button
Press the Info button
Press the Right Arrow button
Press the Left Arrow button
Press the TV/VIDEO button
Unplug your receiver for 30 seconds.
You will get a confirmation message.

Model 5100 also has a procedure to reset/erase the hard drive:

With the remote control press Menu
Press the number 6 button
Press the number 3 button
Press the Info button
Press the Right Arrow button
Press the Left Arrow button
Press the Stop button
Unplug your receiver for 30 seconds.
You will get a confirmation message.
Note that Master Resets also delete any previously entered passwords and thus is very useful for those who have forgotten them.

Broken Remote Control

If your remote control no longer operates, you can call BEV for a replacement unit for approximately 99,00$. An interesting alternative is also available. The One-for-All model URC-5651 is priced at only 15,99$, for further details see: http://www.oneforall.com/index2.html and browse to "Universal Remote Controls" then "Mainstreamline" and choose model URC-5651.
**EEPROM 24LC16B Replacement**

If you have damaged your receiver's 24LC16B EEPROM you can purchase them at the following URLs:

**USA**

**Canada**
search for part # 24LC16B/SN

To do this you will have to program the new EEPROM using the 24 bytes of your TSOP from the following starting addresses:

- 0x00FC8 for models 1000, 3100, 3000 and 4000
- 0x07FFA8 for models 2700 and 3700
- 0x1FFFA8 for models 4700 and 6000
- 0x3FFFA8 for model 5100

**BEV Channels**

An updated channel listing is maintained by a Sattech member and can be download or browsed at the following URLs:

- [http://www.bevlisting.com](http://www.bevlisting.com) (pdf)

A 14 day TV Guide for both BEV and Dish Network can also be browsed at:

- [http://tvlistings2.zap2it.com](http://tvlistings2.zap2it.com)

Simply enter your Postal/Zip Code, choose your provider and browse away.
ATMEGA TROUBLESHOOTING

If you receive an error message or are faced with a black screen only, here are a few possible causes:

- Make sure you are using a "Straight Through" DB25 to DB25 cable.
- Try rebooting your computer in Windows "Safe Mode" and reprogram your Atmega board with the Jeepers software. If this works, it is most likely that a conflict with other hardware exists on your computer.
- Verify all soldering points on the Atmega.
- Verify that your BIOS LPT port setting is in ECP or bi-directional mode.
- Make sure you are using the NawapoM0.0f software for BEV.
- The jumper is in place when you program.
- As of writing this manual, Atmega boards do not work on models 3000, 3500, 4000 and 4500. For model 6000 use the same programming method using NawapoM0.06k with an 18.432 Mhz crystal.
- In the Network field choose "Both" instead of "ExpressVu"
- In the Board field make sure you have chosen the appropriate Atmega crystal setting.
- Make sure your receiver power cord is plugged directly to a power outlet and not through a powerbar.
- With Atmega boards the boxkey number is mandatory.
- Make sure your jumper conducts properly.
- In the Atmel menu of Jeepers choose "Atmega128" then "Fuse Lock Settings" and make sure to check "CKOPT" and "M103". If your board still doesn’t work, uncheck these values only and no other indicated values.

Saving Your AVR’s Configuration

After configuring your AVR with the appropriate information you will no doubt want to save this for future use. From the Jeepers "File" menu choose "Save Configuration". If your AVR needs to be reconfigured, reload the saved file by choosing "Load Configuration" from the "File" menu and update the needed information.

AVR Programming Errors - Initialization Failed & Others

If you are receiving errors while programing the AVR, here are a few things to check:

Make sure your cable is a "Straight Through" type DB25 to DB25.
Reboot your PC in Windows Safe Mode and try to program your AVR again. This will ensure that no conflicts are preventing communication to the AVR.
Make sure that your Atmel microprocessor is installed correctly. If you hold the AVR in your hand with the DB25 connector towards the left, pin1 marked with a circle and triangle should be in the upper left of the IC socket.
Inspect all soldering points on the AVR to make sure they don’t overlap causing short circuits.
Verify that your BIOS LPT port setting is in ECP or bi-directional mode.
Black Screen

Many reasons can cause you to have a black screen with or w/out sound and channel guide, here is a list compiled from various discussion boards:

Make sure your AVR is inserted in the receiver with the DB25 connector facing up.
Verify all soldering points on the AVR
Make sure that your Atmel microprocessor is installed correctly. If you hold the AVR in your hand with the DB25 connector towards the left, pin1 marked with a circle and triangle should be in the upper left of the IC socket.
Verify that you have correctly programmed the AVR with the valid Public Key and have checked Key0 or Key1.
If you have chosen the Married Sub option, make sure your CAM is in the AVR.

AVR PCBs

If you wish to purchase virgin PCBs, they are for sale at the following URLs

USA
http://az-electronics.com

USA & Canada
http://www.hightechhobby.com

TSOP Read/Write Using The JTAG Connection

It is possible to reprogram the TSOP via the connector under the receiver. Here is the procedure:

PROCEDURE TO READ YOUR TSOP
1. Connect your JTAG to the PC parallel port and to the receiver connector.
2. Start your computer.
3. Power on the receiver.
4. Start the Jkeys software.
5. In the "Start" field enter your "Starting Address" and "Bytes" value found in the table below according to your model receiver.
6. Click on the "Save Mem" button and a dialog will appear asking you where to save the data.
7. Once saved, power off your PC and receiver and disconnect the JTAG.
8. If your receiver has two TSOPs, repeat this procedure for each.

<table>
<thead>
<tr>
<th>MODEL</th>
<th>STARTING ADDRESS</th>
<th>BYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>2700</td>
<td>7FF80000</td>
<td>80000</td>
</tr>
<tr>
<td>3700</td>
<td>7FF80000</td>
<td>80000</td>
</tr>
<tr>
<td>4700</td>
<td>7FE00000</td>
<td>20000</td>
</tr>
<tr>
<td>3100 ic23</td>
<td>1FC00000</td>
<td>200000</td>
</tr>
<tr>
<td>3100 ic22</td>
<td>IFE00000</td>
<td>200000</td>
</tr>
<tr>
<td>5100 ic U7</td>
<td>7FC00000</td>
<td>400000</td>
</tr>
<tr>
<td>5100 ic U6</td>
<td>7F800000</td>
<td>400000</td>
</tr>
<tr>
<td>6000</td>
<td>7FC00000</td>
<td>20000</td>
</tr>
<tr>
<td>6000</td>
<td>7FE00000</td>
<td>20000</td>
</tr>
</tbody>
</table>
PROCEDURE TO WRITE TO YOUR TSOP

1. Connect your JTAG to the PC parallel port and to the receiver connector.
2. Power on your PC.
3. Power on the receiver.
4. Start the JKeys software.
5. Click the Flash Info button and a dialog will appear.
6. After about 5 seconds, disconnect pad#1 of the JTAG connector from the ground.
7. Immediately click OK in the JKeys dialog window, a page allowing you to reprogram the TSOP will appear.
8. Click the Erase Flash button.
9. Click on the Write Flash button and locate the previously saved .bin file.
10. Once completed, close JKeys, power off the PC and receiver and disconnect the JTAG.

Model 6000 Procedure:

Connect your JTAG to the PC parallel port and to the receiver connector.
Power on your PC.
Power on the receiver.
Start the JKeys software.
Click the Flash Info button and a dialog will appear.
Power off the receiver for 30 seconds and power on again.
Immediately click OK in the JKeys dialog window, a page allowing you to reprogram the TSOP will appear.
Click the Erase Flash button.
Click on the Write Flash button and locate the previously saved .bin file.
Once completed, close JKeys, power off the PC and receiver and disconnect the JTAG.

For real enthusiasts, satFTA a senior member of many discussion boards has compiled a list of information pertaining to reading/writing TSOPs available at the following URL:


Windows 95 Issues

AVR programming software such as Eepedit have problems running on Win95. This can be fixed by downloading a missing file from the following URL:


Satellite Positioning

If you wish to find out a satellite's positioning in relation to your geographic location, the following URL may help you:


BEV's satellite is named NIMIQ1 and those used by Dish Network are called Echostar

Don't forget to do the Geographic and Magnetic North correction.
**Receiver & CAM Numbers Validation**

You will notice that by pressing the "SysInfo" button on your remote control that your receiver and smartcard numbers always appear in the following format:

R00 1234 4321-XX
S04 1234 4321-XX

Recently a tester "h0rhay" has found a way to calculate the value of these numbers. These values are used by BEV to determine the validity of your receiver and CAM numbers.

Let us suppose that your SmartCard number is S04 5212 3456

Take 0452123456 and devide by 2300
452123456/2300 = 196575 with a remainder of 956

Take the remainder of 956 and devide by 100
956/100 = 9 with a remainder of 56

Add these two values of 9 and 56
9+56=65

The SmartCard number you will get by pressing the "SysInfo" button will be
S04 5212 3456-65

If the final value of our example (9+56) would of been greater than 100, you would then subtract 100 from the value. For example if the number would of been 115 we would of calculated 100-115=15 which would give us the validation number.

**AVR Resellers**

Should you decide to buy an AVR from an online reseller, it is of the upmost importance to order using COD. This will avoid having to use your credit card and guarantee anonymity. Our web site has a Sponsor section with retailers who give full support for users of the guide. We also recommend to order products from your country of origin, this will avoid any custom/duty fees.

**SEE:**

http://www.maestra.ca/english/sponsors
CONCLUSION:

We hope this guide has helped initiate you to the hobby of satellite testing. The manual will be updated for the benefit of the entire community and can be downloaded from our web site at http://www.maestra.ca. Your comments, suggestions, additions and corrections are most welcomed. Please see our suggestion box at: http://www.maestra.ca/english/suggestions.

This guide has been inspired in part by the numerous tests and discussions of members from these respected web sites:

Sattech http://www.sattech.net/
EvuAvr3 http://www.evuavr3.com
Innermatrix http://www.innermatrix.net
Promotional-Solutions http://promotional-solutions.net
Interesting Devices http://id-discussions.com/vBulletin

We would like to thank all of these members and web sites.

I would like to extend special thanks to Baja, and Jugglor.

Maestra
Updated 16 June 2002