

# SECA2 Newbie FAQ by pop-rock v1.2 [08-04-04]

Translated by CJ

This FAQ has been written for people who are not experts in the Mediaguard encryption system. This overview will hopefully provide an introduction to more complex documents, allowing readers to understand the terminology and the base mechanisms that are behind SECA2. Hopefully it will stop people coming onto the forum and asking the same basic questions time and time again....or possibly not!

This FAQ does not replace other more technical documents that are found on the net. It is actively encouraged that readers also study the FAQ of *IconofCoil* and "Scrittura Controllata" released in Italian by *Bramino* (or in Spanish with the title: "Escritura Controlada"). It is also worth consulting the threads on the various forums discussing the technical side of SECA2 (DigitalFreeSat, Tiranniadigitale etc.)

Familiarity with the SECA2 system requires study, once you have studied then you can contribute!

## Basic Concepts

When the card is activated by the supplier\* the following keys are created: MK01, OPK 0C, OPK 0D and OPK 0E, (MK00 is not created or changed) (where MK stands for Master/Management Key and OPK stands for Operating Key). In some cards (usually those which are pre-activated) MK02 and MK03 are also present, but they are of no interest to us. Generically when a card leaves the manufacturers it has the following MKs defined: MK00, MK 02, MK03. Commonly the activation sent from the supplier\* erases the MK02 and MK03 before building the MK01 and OPKeys, this is the old system they used in SECA1 when the MK02 and MK03 of each card were always the same! MK02 and MK03 could be used as a "backdoor" to open the cards. SECA2 activations have no reason to erase MK02 and MK03 because they differ from card to card. Why they do that? Nobody knows!

Every key (Master and Operating) is composed of 8 bytes (for the experts: remember that this FAQ is for newbies therefore I will not mention that the keys are really 16 bytes, 8 primary and 8 secondary! Bugger! I mentioned it! From now on this FAQ is for newbies!! Thanks!).

\*Note: TV supplier is referred to as "Grande Fratello" or GF in Italian meaning Great Brother (this is the way we call the Provider SKY in Italy).

Currently there is no easy way to dump the keys directly from the cards and know their decrypted value. When programs obtain values for the keys (when the programs read the bytes besides the records 8x) they are encrypted... or... best: they are MASKED to not letting us know their decrypted values, which is of no use in decrypting TV.

At the time I wrote v1.1 of this FAQ (October 2003) there was not the knowledge we have now, so after 6 months we (in Italy and Spain) are now able to READ the following keys from our cards:

MK01 + Operative Keys 0C, 0D and 0E.

How can we do it now? First of all, please understand that I didn't use the word "DUMP" but I used the word "READ". We are now able to decrypt the activation instructions sent from the supplier, so we can READ the keys it writes to our cards.

To do that we use two separate processes called: **de-SSE** step and the **de-SE** step.

An instruction sent by the supplier has the following features:

1. its final 90 bytes are completely encrypted with the RSA algorithm. We call the instruction encrypted in RSA as "Ins under SSE".
2. After we will decrypt the SSE from the instruction, we won't see the commands in clear because they are still encrypted in SE.

We look at the **de-SSE** step now:

To decrypt the "Ins under SSE" we use the following scheme:

$$Mc = (Md \wedge Exp) \text{ Mod } N$$

where:

Mc is the Encrypted Message (the last 90 bytes of the instruction we have logged)

Md is the Decrypted Message (the last 90 bytes of the message without the RSA encryption)

Exp is the Public Exponent of encryption (this consist in 6 bytes)

N is the Module of the encryption (this consist in 90 bytes)

Both Exp and N are contained within each cards EEPROM. Exp and N are the same from card to card of a same supplier, but they differ from card to card of two different suppliers.

i.e. Italian cards and Spanish cards use different Exp and N to each other.

All the Italian cards use the same Exp and N.

All the Spanish cards use the same Exp and N.

TUTV card will have different Exp and N to Italian and Spanish cards....got it!

The Italian and Spanish EEPROMS have been dumped thanks to so-called UNLOOPERS or GLITCHERS that goes at frequencies from 100Mhz to 300Mhz and trick the card into exposing its contents.

The dumps themselves are not yet available for the public domain, but the value of the RSA Keys (Module N and Exponents) have been discovered inside pirate cards released on Titanium Cards platform.

Now we look at the **de-SE** step now:

After we have decrypted the SSE from the instruction we find that that the bytes WITHOUT THE SSE are still UNDER SE because they are encrypted with two important factors:

1. The instruction is encrypted with the value of the key that is signing the command
2. This encryption uses a Hash Table that resembles the 3DES Algorithm.

There are 3 tables on each card. Two tables are in the EEPROM: Table Bx and Table Fx and have been dumped out. One table is in the ROM and has not yet been dumped out at this date (8th April 2004)!

It is impossible to write now all the steps to do to release the de-SE procedure and it is a Newbie FAQ after all! Just consider that it is used a system that divide the instruction into separate octets and decrypts them one by one. At the end we will obtain (finally!) the instruction WITHOUT SE and we can read the value of the nano commands inserted in the instruction.

### Unencrypted Data



- ATR (Answer To Reset), conforms to the ISO9660 standard and allows the Conditional Access Module (CAM – located in your set top box etc) to identify the smart card. We are particularly interested in the bytes of data between 96 and 0E (e.g. for TUTV card - 96 70 70 67 0e) as these allow us to determine the card version. The 10<sup>th</sup> byte of the ATR (the one before 0E) gives us the revision number reversed (in TUTV case 7.6).

In Italy there are two types of card: v7.0(a) released by the supplier in May 2002 and the first card to be released with the SECA2 system. These cards were white in colour and are commonly referred to as “bianchine” in Italian. There were several bugs found in this card and the supplier decided to release a new card referred to as v7.0(b) in March 2003. The new card was also white until August 2003 when it changed to a pale blue colour, hence the name “azzurrine”.

- Unfortunately there is no way to immediately distinguish between v7.0a and v7.0b since both cards have the same ATR (96 70 70 07 0E). They can be distinguished by sending an instruction to exploit a bug in the v7.0a card where it responds with 90 00 and the v7.0b card responds with 9024. The v7.0a cards are in fact subject to the “reset” and “36/38” bugs whereas the v7.0b variant is not.
- Startup Record: This is one of the first values which the decoder requests in the initialisation of the card. If the startup record has been annulled the decoder will give the message “Please Insert Smartcard”. In previous implementations of SECA it was possible to rewrite the startup record to all zeros with an 0x80 at the end, this is not possible with SECA2. The only thing that can be made is a blocker which reports a valid startup record to the decoder.
- Dates: The date information defines the expiry date of the card. Each month a new operating key is issued by the supplier (it writes the 0C or the 0D, while the 0E still remains the same from card to card) and the expiry date of the card is also updated.....unless you have not paid your subs!!
- Provider ID: This represents a group of data defined by the Bitmap, PPUA and keys.

There are typically 5 providers for every card. The first one is defined as the main provider or provider SECA (Ident 00 00) with its keys you are allowed to vary or to add other parameters to all the secondary providers. Theoretically each card can hold

## SECA2 Newbie FAQ by pop-rock

16 secondary providers, but only 4 are normally active. In Italy 00 70, 00 71, 00 72 and 00 73 are the provider IDs. In the UK we have only 1 active secondary provider ID of 00 A7 which refers to TUTV.

- **BMP or PBM (Package Bit Map):** defines which channels the card is allowed to decrypt. The data is comprised of 8 bytes with each bit defining a particular channel, a 0 prevents channel viewing while a 1 permits viewing, hence a bitmap with value of all 1's (FF FF FF FF FF FF FF FF) would allow all channels to be viewed except pay per view (PPV).
- **UA (User Address) or serial number:** this is the only value that is unique to each card. The decimalised version of the UA is printed on each card beneath the bar code. The UA is normally referred to as a string of 4 bytes for convenience e.g. AA BB CC DD.
- **PPUA (Program Providers User Address) :** This is a value of 4 bytes where the first 3 bytes correspond to the Group Shared Address (SA) and the last byte represents the Customer Word Pointer (CUSTWP or CWP). Each group defined by the SA receives the same update of operating keys through a C1400xB15C message, this can include a maximum of 256 cards. Inside this command the F0 mask defines which card in the group should receive the update of operating keys. This mechanism allows the supplier to prevent people who have not paid subscription from being updated for another months viewing.

## Key Updates

The OPK (Operating Keys) are updated each month, in Italy the key updates are generally transmitted on the first Monday of every month and are transmitted each day until the end of the month. The 0E operating key always has the same value but is updated the same as the 0C and 0D keys. If you have not paid your subscriptions your CUSTWP will not be included in the update instruction and hence your card will not receive the required update.

The active key alternates each month between 0C and 0D. For example, if the current key in use is 0C then key 0D will be for next month. In practise we have the keys on the card one month before it is used in the data stream. Consequently every OPK remain on the card for 2 months before being replaced by a new one.

The OPK allow the card to decrypt the CW (Control Word) that arrives every 15 seconds in a C1 3C message. Once the card has decrypted the control word the DW (Decrypted Word) can be sent back to the decoder in the form of a C1 3A message.

The updates are sent to every groups SA (Shared Address) signed with the MK01 key which is the same for all cards in the group. I repeat: all cards with the same group SA have equal MK01 keys! Note that these cards have ONLY the MK01 and Group SA in common and nothing else!! The MK00 is varied and is unique to each card. Therefore, as an example, if I have two cards with a PPUA pertaining to the same group i.e. 11223301 and 1223398 they will have the same MK01 (clear enough ;-))!! If one card had a valid subscription but the second card did not the second card would not be able to receive the key updates unless the CUSTWP had been changed on the second card since this forms part of the instruction and

hence the signature.

To summarise: the MK01 and SA are not unique. In order to receive the key updates the card must have a valid MK01, SA and CUSTWP.

There have been lots of questions on the forums of the form “I have written a known good PPUA of a card in place of an unsubscribed PPUA but I am unable to receive the key updates, why?” The reason is that the key update message is signed with an MK01 that is common to all the cards in the group with the same SA i.e. each group has a different MK01. The card which has had the PPUA overwritten is most likely from a different group and therefore has a different MK01, hence it cannot decrypt the key update message correctly (usually a 90 02 response will be given).

Another frequent question is : “Some message has cancelled my MK01, can I recover it from the logs or recreate it some way?” There is no way to recover an MK not even if the logs are available at the point it was cancelled. The only way to recover your own MK01 is to re-send the activation or remapping (change in PBM) instruction as this is signed by the MK00 and it will rewrite the MK01, PBM, DATES, OPK 0C, OPK 0D and OPK 0E.

Hypothesis 1: You have cancelled MK01, but conserved MK00 and you have access to your activation log. However, you are not a subscriber so you cannot telephone the supplier and ask for a change to your package which would restore your MK01. Sending the activation will rewrite all the required information including MK01 but the date information and operating keys will be from when the card was activated. You will therefore have to find logs of each months updates and apply them one by one to return the card to the current date. Obviously you will also have to change the CUSTWP since the original has been theoretically deactivated. The date can be changed to any time in the future, the import thing is that it is not more than two months older than the key update we want it to process. It is possible, using the bug, to set the date (for example) to 23 July 2089 even though this is far in the future the processing of the updates is only cancelled for dates in past.

Hypothesis 2: You have cancelled MK01, but conserved MK00. Unfortunately you do not have access to your activation log and you are not a subscriber. Without the activation log you will be unable to resurrect MK01 and therefore you will be unable to update the card with the OPK.

Hypothesis 3: You have a cancelled MK01 but still conserved the MK00 and you do not have access to your activation log, but you are still a subscriber. It is most convenient to telephone the supplier and make a complaint about lack of service or ask for a change in package. It is most likely that the supplier will send a new activation message which will rewrite MK01.

Hypothesis 4: You have cancelled MK01 and MK00. Even is you have access to your activation log you cannot use it because this is signed with MK00. Your card now makes a nice ice scraper!!

To these hypotheses I add one special one:

Hypothesis 5: You have cancelled MK00, but MK01 is still present. The key updates will continue to be decoded correctly since they are signed with MK01. You may be in trouble in the future if the supplier wanted to move your card to a different group for example since

your card will no longer decode activations, reactivations or remappings since they are all signed with MK00.

### Activations (C1400xB061 until 27/01/03, after C1400xB063)

The activation instructions are sent approximately 3 times in the first hour after the activation request and then a further 3 times in the next 24 hours. If you have not managed to log the activation in this time then you will have to telephone the supplier to ask for a new activation, even if this means requesting a remap at the same time.

The activation inserts UA (Unique Address) and MK00. The UA is, um, unique! It does not work on the same principle as the PPUA where there are 256 cards in a group. This is because if there were sister cards they would all receive the same activation and deactivation instructions when one of the group did not pay subscription for example! The MK00 also varies from card to card and they are not the same for groups of cards either (unlike the MK01).

Therefore, it is stupid to ask: "I have not found the log of my activation for my UA of type CC CC CC A1, but I have found a log of activation for another UA which is very similar CC CC CC A2, will this be ok? The answer is NO! Only the supplier can create the activations for the simple reason that these commands are created from an algorithm that is not known.

### Remapping

Sometimes, when many of the subscribers CUSTWPs in a SA are inactive the supplier will move the remaining subscribers to a new SA. This can happen when the subscriber asks to change their package or as part of a reorganisation. When the subscriber is moved to a new group of 256 cards the MK01 must be updated in order that the card will continue to decrypt the OPK updates each month. The subscriber will actually rewrite all the MK01 keys for the new group so each of the 256 cards in that group have a different key.

This means that commands logged with the old MK01 can become unsuitable since the command cannot be correctly decrypted with the new MK01. MK00 is not modified during the remap and hence logs of activation previous to remapping are still useful for the bug!

The only way "to work" on a card that has been remapped and which you do not possess the log of Pre-Black Monday activation, is through the use of the Universal Instruction. That is, an instruction of the form C1 3x. These instructions, signed with the key 0E, allow us to overcome the countermeasure (defined "CETRIOLO") adopted by the supplier after 27<sup>th</sup> Jan 2003 (also known as Black Monday). The countermeasure was a response to the publication of the 36/38 bug and was implemented by adding 2 bytes (16 0B) to the key update and activation/remap/deactivation instructions.

### Deactivation (C1400xB05C)

The deactivation instruction is used to cancel all the keys except the MK00. This is so that the supplier can use it to reactivate the card at some point in the future via an activation instruction. In addition to removal of the keys (MK01, 02 and 03 if present and OPK0C, 0D



and 0E) the date information is also reset, typically to 01 Jan 1991. Often the PBM is also reset to a value of all zeros.

### Terminology

- BM (or Black Monday) : This refers to 27<sup>th</sup> Jan 2003 when the supplier put into place the countermeasure known as “Cetriolo”.
- RBug (or Reset Bug or sometimes just “the bug”) : This refers to a programming error in the firmware of the first cards which allowed a positive response (90 00) by sending repeated reset to an instruction that would normally respond with (96 00) for example. The RBug was the origin of all the hacks we did in Italy on our cards. The cards that cannot support RBug are still UNOPENED and they are under strict study up to this date! That's why the V.7.0(B) in Italy, the V.7.1 in Poland and France, the V.7.3 in Nederland and so on... have not been yet hacked! (Or at least they have not been PUBLICALLY hacked :-))
- Cetriolo : Countermeasure “software” put into effect after Black Monday from the supplier to resolve the Reset Bug. This countermeasure has since been overcome by means of the Universal Instruction.
- Gronoco : Countermeasure “hardware” issued to plug the holes in the first set of cards. The gronco is one patch of the firmware released in the v7.0b cards. The patch does not allow us to trigger the Reset Bug/Universal Ins and is therefore unhackable for the moment.
- Moderators : Common people like all users of the forum who train in the subject matter of the forum in question. Often moderators do not know any more than other special users (so-called gurus). The moderators carry out their task FREE OF CHARGE.
- Pappapronta : Someone who is unwilling to learn and only wishes to use some program or other to get free TV.