# Frequently Asked Questions

- **SECA questions**
    - How is a subscriber authenticated?
    - What's the difference between descrambling and decrypting?
    - Where is the encryption&decryption in SECA?
    - Where is the subscriber entitlement?
    - What about the PPV?
- **Can I fool SECA by...**
    - changing the subscription termination date in SECA ins 0x12?
    - changing the current date in SECA ins 0x3C?
    - changing something in SECA ins 0x40?
    - changing the serial number in SECA ins 0x0E?
    - changing the smartcard address in SECA ins 0x12?
- **The Three Mac's (software)**
    - Do your programs work with other CAM's too?
    - What about the baudrate?
    - Can you write versions for Win 3.1?
    - How's the NT support?
- **General questions**
    - Nice site. Are you planning to study other conditional access systems too?
    - Does my season work with my decoder? What do I do about it?

# SECA questions

### How is a subscriber authenticated?

At decoder startup the smartcard needs to respond to several instructions. Look at the section "SECA in Practice" to see the startup and authentification sequence of the CDV, CSN, CSD and D+ systems.

### What's the difference between descrambling and decrypting?

First you should read the information on this page. Looking at the DVB standard you can see that it includes the scrambling. The **scrambling** is the actual encrypting of the video and audio information, the MPEG-2 stream. They reached an agreement about the scrambling method, commonly referred to as the Common Scrambling algorithm.

This means that ALL DVB compliant Digital TV systems use the SAME scrambling algorithm. It is a combination of a 64-bit block cipher followed by a stream cipher algorithm. The technical details of the Common Scrambling algorithm are secret and only made available under a Non-Disclosure-Agreement for access control hardware manufacturers.

The Common Scrambling algorithm needs a start seed. This start seed or key is commonly referred to as the Control Word (CW) . The CW is sent to the decoder in an encrypted way. This is the **encryption** we speak of. For the encryption no agreement was reached with several different CAM systems as a result. So MediaGuard is only one of several possible conditional access systems. Others include Irdeto, Viaccess, Conax and Cryptoworks. Remark that these or **digital** conditional access systems. Other popular analog systems include D2MAC (Eurocrypt) and Videocrypt.

### Where is the encryption&decryption in SECA?

Have a look at the SECA instruction list. You'll see that the instructions 0x3A and 0x3C handle decryption. INS 0x3C (ECM) contains the encrypted Control Word (together with some access control) and INS 0x3A is used to get the decrypted Control Word. It's this access control in the ECM that can shut you out a channel or even a complete bundle or bunch of channels.

### Where is the subscriber entitlement?

When does your subscription end? Which channels can I view? Is my card dead or alive? All the answers to these questions are set via the 0x40 instructions. These are the Entitlement Management Messages.

### What about the PPV?

You can find some information and two PPV scenarios here.

## Can I fool SECA by...

### changing the subscription termination date in SECA ins 0x12?

Remember that this instruction goes from smartcard to decoder. If you were to change the date (for example by using MacSmart), the decoder will believe you. In other words you're fooling the decoder, not the smartcard. If your card would get a 0x3C instruction with a date higher than the subscription termination date, it will refuse to decrypt the ControlWords. This means instruction 0x3A will return all 0xFF's, thus invalid CW's.

### changing the current date in SECA ins 0x3C?

This instruction is cryptographycally signed. This means that you **can't change anything** in the instruction without reapplying the signature. The problem is... the signing algorithm is secret, furthermore you'll also need a secret key. This secret key is the parameter for the signing algorithm. So you can **see** but you can't **touch**:-)

### changing something in SECA ins 0x40?

And what exactly would you change? These instructions, while being the most interesting ones, are the most protected ones. They are completely encrypted. Again with a secret algorithm parametrized by a secret key. In this case you can't even see anything, let alone make some changes...

### changing the serial number in SECA ins 0x0E?

So you think filling in the serial number of a fully enabled card will get you all channels? Too bad... This will not work because the serial number is not used for addressing a specific smartcard. I mean that the subscriber specific 0x40 instructions (the ones containing the access rights, remember?) are sent to a so called "smartcard address" located in instruction 0x12.

### changing the smartcard address in SECA ins 0x12?

Keep trying:-) The 0x40 instructions (or the EMM's) that are subscriber specific, are encrypted with subscriber specific secret keys. This means that by changing the smartcard address, you're card will receive 0x40 instructions which it **can't** decrypt...

## The Three Mac's (software)

### Do your programs work with other CAM's too?

They should work with a lot of other smartcard applications, including other CAM systems. All you need to do is find out the correct serial I/O settings by experiment. Some tips:

- Try looking for the 5 byte smartcard instruction format, followed by the INS acknowledgment.
- Look for the ATR on reset, it should end with 90 00.
- Don't forget to try the Inv checkbox.

When this is done, start logging the traffic between the smartcard and the decoder. Doing this you get an idea of the smartcard instructions used. You can now create a SmartCard Configuration file using either MacSmart or MacTalk.

### What about the baudrate?

Some decoders use 9600 baud, others use 10000 baud, others even use another baudrate. Experiment!

I got a mail from someone that 10000 baud didn't work and that 10472 baud was required. This can vary from smartcard application and computer. 10000 baud worked for me. The baudrate for the serial COM port is configured in this way:

- 9600 baud ==> 115200/9600 = 12 giving a divisor of 12 to be loaded in the Divisor Latch.
- 10000 baud ==> 115200/10000 = 11.52 giving a divisor of 11 to be loaded in the Divisor Latch.
- 10472 baud==> 115200/10472 = 11.000764 giving the same divisor of 11.

The important thing to see is that it's not the baudrate that's important, but the divisor! Since 10000 and 10472 give the same divisor it **should** give exactly the same result. **BUT,** I assumed that 11.52 was rounded downwards, if it was rounded upwards you would get 12 giving 9600 baud! Get my point? **To be sure of the divisor it would indeed be best to either select a baudrate of 9600 (12) or 10472 (11).**

I've noticed that WinNT does not accept 10000 baud, you have to set 10472:)

### Can you write versions for Win 3.1?

Nope.

### How's the NT support?

For the moment NT does not like my threads. You can use the programs but they will not terminate correctly. Also do not use the Restart option, just quit and start. Hey, don't shoot me: after all, they are free:-)

## General questions

### Nice site. Are you planning to study other conditional access systems too?

No, not for the moment. You're always welcome to make a site yourself !?!

### Does my season work with my decoder? What do I do about it?

Read this.