Monitoring Conditional Access Systems

Introduction
A Conditional Access system is a key component for most digital TV operations. They secure the operators' investments by encrypting the signals and ensures that all customers have to pay in order to watch TV. Conditional Access systems (CA systems) are highly proprietary and are surrounded by a lot of secrecy. While most operators have highly skilled personnel with a lot of knowledge in MPEG, DVB and networking, the knowledge of the CA systems is usually limited.

Conditional Access systems are complicated and are unfortunately a frequent source of problems for Digital TV operators. Encryption is used in every aspect of the CA system which makes it hard to find the cause of problems. The problem descriptions from the end users are often of the type “My screen is just black” or “Why does the TV say No Access?”. This does not give the operator many clues for solving the problem.

The operators usually have analysers to find the cause of 'normal' signal problems but the tools to debug Conditional Access systems have been lacking. Most analysers and monitoring equipment follow the ETSI TR 101 290 standard promoted by the DVB organization, but this specification does not cover Conditional Access at all. Conditional Access related problems usually result in finger pointing instead of useful problem solving. Is it a problem with the Conditional Access system, or the STBs? The smart cards or the multiplexer? Maybe the descrambling at the input of the head end has failed, or perhaps there is an network problem? Without the right tool it is difficult for the engineers to know.

Having an analyzing product which can shed light into the black magic of the CA Systems make finding the cause of the problems much easier. Having a monitoring product which finds the problems with the Conditional Access system long before the customers notice problems will save the operator money and avoid problems with dissatisfied customers.

Like most other monitoring applications it is not practically possible to cover absolutely all possible problems affecting any subscriber. However by relatively simple means it is possible to monitor and detect common problems which are likely to occur in a Digital TV system.

The techniques described in this article applies equally well regardless of the transmission medium used to send the Digital TV signals. Monitoring of the Conditional Access systems is currently in use by a large number of operators transmitting Digital TV over many different technologies:

- IP-TV, for instance fiber to the home and DSL operations
- QAM for cable TV networks
- COFDM for terrestrial networks
- QPSK and DVB-S2 for satellite networks
- ASI for signals used in the head end
Brief Description of Conditional Access Systems

**Scrambling**

In Europe all Conditional Access systems for satellite, terrestrial and cable broadcast use the Common Scrambling Algorithm (CSA) to perform the actual encryption and decryption of the TV signals. In the CSA specification this is known as scrambling and descrambling. Some vendors focusing solely on Conditional Access systems for IP-TV have chosen other scrambling algorithms but CSA remains the de facto standard.

The clear signal is fed into the scrambler which encrypts using the Control Word. The descrambler uses the same Control Word to recreate the original clear signal.

The clear (not encrypted) signal is fed into a scrambler which encrypts the signal using a random encryption key called the Control Word (CW) according to the CSA algorithm. The descrambler decrypts the scrambled signals by using the same Control Word to reproduce the clear signal.

In a normal DVB system, the scrambling takes place in a multiplexer or an IP Streamer, while the descrambling takes place in a set-top box (STB). The Control Word used for scrambling is chosen randomly. This is normally done by the device performing the scrambling.

The Simulcrypt specification as well as the MPEG and DVB specifications regulate how the information is sent in the signals and how the information needed by the CA system is to be transmitted.

For security reasons the Control Word used for scrambling is changed regularly, usually every 10 seconds. The transport stream header contains two scrambling control bits which indicate which Control Word are to be used for descrambling, normally denoted Odd and Even. This allows the Control Words to be changed without causing any descrambling problems.
ECM

The most important task for the Conditional Access system is to transmit the Control Word needed to descramble the signal to the STB in a secure manner. The Control Word is placed in a message called an Entitlement Control Message (ECM) which is encrypted in a proprietary way and then inserted into the Transport Stream.

Most Conditional Access systems use smart cards which are inserted into the STB to handle the security, but some CA systems use a software component in the STB instead of a smart card. The smart card receives the ECM associated with the TV channel, decrypts the ECM and sends the Control Word to the STB so that it can be used to descramble the signal.

The clear signal is fed into the multiplexer that encrypts using the Control Word. The current and next Control Words are sent to the Conditional Access system ECM encryptor which will create an encrypted ECM containing the current and next Control Words. The ECM is then returned to the multiplexer that inserts it into the transport stream.

The contents of the ECM varies between the different Conditional Access vendors but typically contains at least the following information:

- Two Control Words. This allows transmitting both the currently used Control Word as well as the Control Word which be used when the scrambling control bits in the transport stream header change.
- Time and date information. This allows the smart card to know what the current time is and to make a decision if the user is allowed to watch the channel or not (most subscriptions are time limited and renewed regularly with EMMs).
- Channel identification. Can be unique for the channel or shared between all channels in a subscription package. The channel identification allows the smart card to look up the channel in its internal access table.

The ECMs are typically repeated every 100 ms so that the STBs are able to quickly start descrambling after changing channel.
EMM

In a Conditional Access system the Entitlement Management Message (EMM) is used to send entitlements to the smart card, for instance information such as “Allow the user to view this group of channels the next month” or “Allow the user to watch this Video On Demand movie”. The set-top box will receive the EMMs and forward them to the smart card for processing. The smart card uses the information in the EMMs to update its internal access control database containing a list of channels and VOD movies the user is allowed to watch.

The EMM can authorize the smart card to allow viewing of a VOD movie for a couple of hours, or one or more TV channels for one or several months to come. When the smart card receives ECMs it will use the information in the smart card’s internal access control database to decide if the user has access to the channel or not. If the user has access to the channel the decrypted Control Word will be sent to the STB which can then descramble the signal.

When the subscriber management system updates the access rights of a customer the Conditional Access system will create a new EMM addressed to the client’s smart card. This newly created EMM will be included in the EMM play out carousel. The carousel continuously sends EMMs to the multiplexer which inserts them into the transport stream.

EMMs are encrypted with a proprietary encryption method known only by the CA vendor. The EMM format is highly proprietary but typically contains the following information:

- Length field which is not encrypted. Specifies the length of the EMM
- Address field which is not encrypted. There are typically three addressing types used for EMMs:
  - Unique. The EMM is addressed to one specific smart card or STB
  - Group. The EMM is addressed to a group of smart cards or STBs
  - Broadcast. The EMM is sent to all smart cards or STBs
- Encrypted part

The addressing field in the EMM allows the STB to filter the EMMs and only send the relevant EMMs to the smart card for processing.
Verifying Correct Descrambling of the Input Signals

Most IP-TV and cable TV operators receive a significant portion of their input signals in encrypted form, often over satellite. The various channels will come from different providers which all have different CA Systems.

The first part in the turn-around of Digital TV signals is to descramble the incoming signals. This is normally done in professional descramblers, or directly in the multiplexers or IP streamers.

The input signal is descrambled correctly and is then scrambled with the operator’s Conditional Access system.

If the input signal for some reason cannot be descrambled the signal will still be encrypted with the original CA system. Then, later in the turnaround process, the signal will be encrypted with the operators own Conditional Access system, causing the signal to be encrypted twice. This will normally cause a black screen for end users and the game of blame can begin.
The descrambling of the input signal has failed and the encrypted signal is fed into the operators scrambler. The result is a signal that is encrypted twice and cannot be descrambled by the set-top boxes.

Descrambling failures are typically caused by one of the following:

- Hardware failure in the descrambler
- Hardware failure of the smart cards which are used in the descrambler
- Smart cards which are not inserted correctly or have been removed
- Smart cards which have not been authorized (missing or incorrect EMMs)
- Scrambling failures of the input signal, for instance missing or incorrect ECMs
- There is some problem with the authorization of the Digital TV operator. Bills which have been sent to the wrong address and have not been paid, expired license agreements or problems with the subscriber management system used by the operator providing the input signals.

The solution to this problem is to monitor the signals after descrambling and before they are re-encrypted. A simple approach is to check that the scrambling control bits in the transport stream packets are set to 0 (not scrambled) to verify descrambling. This information is unfortunately misleading as descramblers often flags the PIDs as not scrambled even if it was unable to correctly descramble the signal. This type of monitoring thus has quite limited value.

To get the monitoring needed it is necessary to analyze the incoming signal in detail, especially the video PIDs. For the best possible checking one should check that the audio and video can be decoded. Ideally the monitoring product should be able to extract thumbnail information from all streams and check audio levels. Detecting picture freeze and also “black screens” are also highly useful. These are problems which often occur when the digital signal is decoded and there are CA errors. This is normally done in a decode-recode process to change the bitrate/resolution of the input signal.
Checking Scrambling of the Signals

Most content is normally scrambled in the head end, but scrambling in the edges of the network is becoming more popular. Scrambling in the edges are most commonly used to insert different local content in different regions and to scramble VOD sessions.

No matter where the signals are scrambled there are many potential problems along the way. This article will discuss the most common causes of problems related to the Conditional Access system.

Verifying the Conditional Access Table

The Conditional Access Table (CAT) is used to signal which PIDs in the transport stream that are used for Entitlement Management Messages. The ETSI TR 101 290 specification specifies some basic checks that are to be performed for the CAT table. These checks only require that the CAT table is transmitted when there are scrambled PIDs present in the transport stream and that the CRC checksum of the the table is correct. There are however no checks that require that the CAT table contain any useful information.

The monitoring equipment should also check that the CAT table contains EMMs for all the Conditional Access systems used to encrypt the signals. The list of CA systems used for scrambling can be detected by checking which CA Systems which are listed in the Conditional Access descriptor in the PMT tables.

Missing EMMs

The Entitlement Management Messages are normally transmitted continuously from the CA System to the Multiplexer or IP Streamer which will insert the EMMs into the transport streams. Normally this is done using UDP or TCP over the IP network, but ASI connections are also used. When the EMMs go missing it is usually caused by one of the following:

- Loss of network connection between the CA System and the Multiplexer. This can for instance be caused by:
  - A network cable that slips out of its port
  - Failures in the TCP/IP stacks
  - Incorrect configuration of TCP/IP settings for the multiplexer or CA system
  - Incorrect configuration of routers

- A failure in one of the CA System servers
  - The EMM playout software has crashed or hangs
  - The EMM database has been corrupted
  - Operating system failure, full disc, denial of service attack
  - Incorrect configuration of the server
• A failure in the multiplexer
  ◦ Failure in the software which receives the EMMs from the CA System and inserts them into the transport stream.
  ◦ The input bitrate is too high for the video signal, so the MUX decides to drop the “unimportant” EMMs in order to squeeze the signal into the allowed bandwidth.
  ◦ Incorrect configuration of the multiplexer.

In a system without CA System monitoring the following is likely to happen when the EMMs go missing:

• Day 1: A customer calls in to say that he has not been granted access to the new channels he ordered. 1st line support takes him through the usual steps for finding the cause of the problem and ends up blaming his smart card. They decide to ship him a new smart card.

• Day 2: Several customers phone and send emails describing similar problems. 1st line support ends up ordering new smart cards for all these customers but they eventually see a pattern and forwards the problem to the rest of the organization.

• Day 3: The first day of a new subscription period. As no EMMs with authorizations for the new period have been sent out all users are welcomed with the dreaded ‘No Access’ message when they try to watch the morning news. 1st line support is flooded by calls. It takes 3 hours before the CA expert to arrive at work, 15 minutes for him to get a cup of coffee and then 2 minutes to fix the problem.

On the other hand, when the EMM traffic is monitored the following will happen when the EMMs go missing:

• Day 1: When the EMMs go missing the monitoring equipment will detect the problem and raise alarms for all affected transport streams. The shift operator calls up the CA expert which is already at his desk with a cup of coffee and he spends 2 minutes to fix the problem. No customers are affected by this short period without EMMs.

To have an EMM monitoring scheme which can detect any conceivable problem with the EMMs is not possible. By having a piece of analysing equipment which generates alarms if the EMM bitrate drops below a configured limit, at least 90% of the error situations can be detected and fixed before they cause any problems for the end users. When measuring the EMM bitrate the rate has to be averaged over a certain period of time. Calculating the bitrate over a 1 second period will generate false alarms as it is quite common for the EMMs to be missing for a couple of seconds. Having a fixed period of 10 seconds is usually sufficient, but for maximum flexibility we recommend having a configurable period. The bitrate limit should also be configurable. Use 1 kbps as a starting point and then increase this limit when tuning the monitoring of the EMM bitrate, but be sure to keep the limit so low false alarms are avoided.
Verifying the Program Map Table

The Program Map Table (PMT) can contain one or more Conditional Access descriptors specifying ECMs associated with the service. The ETSI TR 101 290 specification specifies some basic checks that are to be performed for the PMT tables. There are however no checks in this specification that require the PMT table to contain any Conditional Access descriptors even if the components in the service are scrambled. If no ECMs are listed in the PMT table of a scrambled service the service cannot be descrambled.

In order to detect descrambling problems the monitoring equipment should require that services with scrambled components must specify one or more ECM PIDs in the PMT table.

ECM repetition and presence check

When zapping to a channel the STB needs the Control Word in order to descramble the content and start decoding. This means that the transmission interval of the ECMs is very important with regard to zapping time (as are the interval of PAT and PMT tables).

An incorrect ECM repetition interval is normally caused by incorrect configuration of the multiplexer or internal problems in the multiplexer.

If the ECMs go missing all together, the STBs are unable to descramble the content and the user is normally presented with a 'No Access' message. Missing ECMs are usually caused by:

- Failed network connection between the multiplexer and the CA System
- Failure of the CA System ECM encryptor
- Mal-configuration of the multiplexer

To check ECM repetition one will first need to find all ECMs for all the services in the signal. Normally the ECMs are signaled by having the Conditional Access descriptor in the program_info section of the PMT table. This makes the same ECM apply to all component PIDs of the service. It is also possible to have different ECMs for different components by having the Conditional Access descriptor in the ES descriptors section for the component in the PMT.

When the list of ECMs has been found one needs to receive all data on the different ECM PIDs and check the interval between the individual ECM packets. The maximum time allowed between ECMs must be configurable by the operator. 500 ms is a good value to start off with, but this can typically be reduced to 130 ms for most systems.

Control Word change check

The Control Word used to encrypt the transport stream packets are changed regularly, usually every 10 seconds. If the Control Words change stops for whatever reason the STBs can use the same Control Word to decrypt the incoming signal until the problem is fixed. This is a serious security issue.

In this situation the viewers can in this situation have access to the channel for a long period of time even if the operator intended for them to lose access, for instance when unsubscribing from a channel package or when the allocated time for a video on demand movie has ended.

More importantly however this makes it easy for crackers to publish the Control Word used to descramble the signal on the Internet allowing everyone, even without a smart card, to watch the TV channels thereby compromising the security.
Control Words that are not updated are usually caused by:

- Problems with the network connection between the multiplexer/scrambler and the CA system. If the signal is simulcrypted with several different CA systems this problem is more likely to happen. It is also more likely to happen if the CA system is not located close to the multiplexer, for instance when using VPN tunnels over the Internet or when doing local encryption in the edges of the network with the CA Servers in the central head end.

- Problems with the Conditional Access systems ECM encryptor. This can for instance be hardware failures, failures related to the operating system or the CA applications running on the server.

- Problems with the multiplexer/scrambler. Can be caused by misconfiguration of the device or problems with the software running on the multiplexer.

By monitoring that the Control Word change regularly the operator can detect these problems long before they cause any problems. In systems without monitoring these problems can go on for weeks or even months before they are detected unless the operator uses expensive manual inspections to check for these problems.

To check the time between the changes of the Control Word it is sufficient to measure how often the scrambling control bits change.

**Require PIDs to be scrambled or to be clear**

After the signal has passed through the multiplexer performing the scrambling there is usually a set of PIDs that must be scrambled at all times and similarly a set of PIDs that must never be scrambled at all. The monitoring equipment should therefore have the possibility to specify a list of PIDs and their scrambling requirements. For these checks it is sufficient to check the scrambling control bits. For scrambling the operator can choose between the following options:

- The PID must always be scrambled. An alarm will be raised if the PID is not scrambled (clear). This can be used either on all PIDs which are meant to be scrambled or for selected PIDs that always must be scrambled, for instance high definition channels where the license agreement states that the content must be scrambled at all times.

- The PID must never be scrambled. An alarm will be raised if the PID is scrambled. This requirement can for instance be used on PIDs carrying middleware to the STBs or content which for legal reasons cannot be encrypted.

**EMM roundtrip time**

A parameter which is interesting for larger Digital TV operators is the EMM roundtrip time. The operator typically wants to use as little bandwidth as possible for the EMM traffic, instead prioritizing better video quality or having an extra channel.

Larger operators have millions of smart cards and a lot of EMMs are needed to be able to authorize all the smart cards for the channels the users are subscribed to. EMMs are normally sent out well ahead of time so for set-top boxes that are always switched on the EMM roundtrip time is not that important. The EMM roundtrip time is however important when the set-top box have been switched off for a considerable period of time (for instance when going on vacation) since the smart card needs to be updated before descrambling can start. If this takes too long it usually results in user complaints. The definition of ‘too long’ will of course vary from user to user, but generally one can say that all EMMs should have been played out within 15 minutes.
The EMM playout carousels often have several different priorities for the EMM. For instance when the customer calls in and purchases access to a new set of channels the EMM will typically be played out at a high priority and repeated frequently. After 12 hours the EMM can then be set to normal priority and be repeated at normal intervals. A week after that the EMM is marked as low priority and is repeated infrequently.

The Conditional Access system vendors are very secretive and do not want to share information about the EMM formats. For monitoring EMM roundtrip time it is necessary to know the format of the unencrypted part of the EMM. This is the same as all STB manufactures need to understand in order to integrate with the CA system. In order to be able to analyze the EMM roundtrip time it is necessary to reach an agreement with the CA vendor and to get access to some of the specifications that the STB manufactures use to implement the CA system in their boxes.

Once the format is known the following approach should be followed to perform the round trip measurements:

- Select a number of EMM addresses for the different addressing types. For instance, pick one EMM address from the transport stream every second for the first 20 seconds of monitoring.
- Receive all EMMs for the selected EMM addresses, calculate and store a hash of the encrypted part of the EMM.
- When an identical EMM is received (same address, same hash) we can measure the round trip time for this EMM.
- When a sufficient number of measurements have been done, statistical analysis can be performed. Some EMMs are only sent once (before they are changed or removed) so one can not expect that all EMMs are repeated. Patterns will be different from CA system to CA system, but one will typically see some round trip times which are low (high priority EMMs), while others have higher round trip times. By grouping similar measurements one can get round trip measurements for the different EMM priority groups.

For larger systems the round trip time can be up to 30 minutes, and can be even longer for low priority EMMs. This means that to get reliable measurements one will have to measure the signal for quite a long time (at least one hour). All other CA measurements described in this article can be done in a relatively short period of time, allowing for round robin operation, i.e. the analysis equipment can analyze all the different transport streams sequentially. If the EMMs are identical on all transport streams (copying the PID from one multiplexer to another) it is sufficient to monitor round trip time on one transport stream, and then rely on EMM bitrate measurement on the others. However if the EMMs are played out separately for the different transport streams it is recommend that all frequencies are monitored in parallel for the best possible results.

**Checking ECM change relative to CW change**

In each PID header there are 2 bits telling the decoder if the Odd or Even Control Word should be used. The ECM normally contains two Control Words. This mechanism allows the ECM to carry both the Control Word currently used and the Control Word which will be used for scrambling the next time the Control Word changes. This ensures that the STB always has the Control Word needed to descramble the content.

If the time the ECM changes is not properly synchronized with the change of the Control Word used to encrypt the signal there may be periods of time when the STB is not able to descramble the signal thus causing black screen occasionally.
For the ECM change the following applies:

- The ECM should not change too early, the STB should have time to descramble all transport stream packets encrypted with the old scrambling key before the key is changed.
- The ECM should not change too late, the STB should have time to get the CW back from the smart card and store this internally before the scrambling of the signal changes.

<table>
<thead>
<tr>
<th>ODD</th>
<th>CW 1</th>
<th>EVEN</th>
<th>CW 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK FOR EVEN CW TO CHANGE</td>
<td>OK FOR ODD CW TO CHANGE</td>
<td>OK FOR EVEN CW TO CHANGE</td>
<td></td>
</tr>
<tr>
<td>USED SCRAMBLING KEY:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ODD (CW 1)</td>
<td>EVEN (CW 2)</td>
<td>ODD (CW 1)</td>
<td></td>
</tr>
</tbody>
</table>

The change of the ECM has to happen a certain time after the Control Word used to scramble the signal has changed. Similarly the change of the ECM has to happen some time before this new Control Word will start to be used to scramble the signal.

Some Conditional Access systems for IPTV have ECMs which only contains one Control Word. In this case the ECM will change before the scrambling control bits change instead of after. The monitoring equipment must be able to monitor this as well as the normal situation where the ECM changes after the scrambling control bits.

**Conclusion**

Until now there has not been solutions available that are able to monitor the Conditional Access system and raise alarms when problems occur. The operators have either used manual inspection routines to detect problems or have let their subscribers find and report the problems. Both these approaches are costly, both in terms of personnel and dissatisfied customers. As monitoring Conditional Access systems are now feasible we highly recommend that all operators monitor their CA systems and fill the missing piece in their monitoring system.

Conditional Access system monitoring should be integrated with the overall monitoring solution. Coupled with full ETSI TR 101 290 monitoring, monitoring of IP and RF transmissions it provides a powerful and complete system monitoring and analyzing for Digital TV. The monitoring solution should also include an NMS system which aggregates errors from all the different analysers placed in the network and displays not only a list of alarms, but also pinpoints where in the network the problem occurred and generates reports showing measurements such as quality and jitter over time so that the operator can detect trends.
Screenshot of analyser monitoring the Conditional Access system.

Rackmounted version of the analyser with IP, ASI and QAM interfaces. ETSI TR 101 290 monitoring and monitoring of Conditional Access systems are supported on all interfaces. The analyser can also be fitted with COFDM and QPSK/DVB-S2 interfaces.