Claims

1. Method to watermark an uncompressed content received at a client device in a compressed form and encrypted by at least one content key (CW), said content key (CW) as well as watermark instruction forming CAS data, said CAS Data being encrypted by a transmission key and comprising at least one signature to authenticate the CAS Data, said client device comprising :

- A Conditional Access Module (CAS) in charge of the CAS Data,

- a Descrambler (DSC) having an input to receive the encrypted compressed content and an output to produce a decrypted compressed content,

- a decoder to convert the decrypted compressed content into uncompressed content,

- a Watermark inserter (201) connected to the output of the Decoder,

- a Secure Activation module (202) connected with the Watermark inserter (201),

- a Secure Element (SE 200) connected with the Watermark inserter (201) and the Secure Activation module (202),

said method comprising the following steps :

- receiving the CAS Data,

- decrypting by the Conditional Access Module (CAS) the CAS Data with the transmission key,

- verifying the signature of the CAS Data, and if the signature is valid,

- transferring the watermark instruction to the Secure Activation module (202),

- transferring the content key (CW) to the descrambler (103) only if the transfer of the watermark instruction was successful,

- transferring the watermark instruction to the Watermark inserter (201),

- enabling or disabling watermarking by the Watermark inserter (201) of the uncompressed content received from the Decoder., in accordance with the watermark instruction, said verification of the signature comprises:

- requesting by the Secure Element (SE 200) a random number (X) from the Secure Activation module (202),

- generating this random number (X) by the Secure Activation module (202), storing it and sending it to the Secure Element (SE 200),

- preparing by the Secure Element (SE 200) a message containing at least the watermark instruction, the random number, and a signature on both the watermark instruction and the random number,

- sending this message to the Secure Activation module (202),

- verifying by the Secure Activation module (202) if the signature is authentic and if the random number is the same as the one sent previously, in the positive event, accepting the watermark instruction, and

- sending a final acknowledgment message to the Secure Element (SE 200) in order to inform the Secure Element (SE 200) of the successful completion of the transfer.

~~2. Method of claim 1, wherein the transfer of the watermark instruction from the Secure Element (SE 200) to the Secure Activation module (202) comprising the steps of :~~

~~- requesting by the Secure Element (SE 200) a random number (X) from the Secure Activation module (202),~~

~~- generating this random number (X) by the Secure Activation module (202), storing it and sending it to the Secure Element (SE 200),~~

~~- preparing by the Secure Element (SE 200) a message containing at least the watermark instruction, the random number, and a signature on both the watermark instruction and the random number,~~

~~- sending this message to the Secure Activation module (202),~~

~~- verifying by the Secure Activation module (202) if the signature is authentic and if the random number is the same as the one sent previously, in the positive event, accepting the watermark instruction, and~~

~~- sending a final acknowledgment message to the Secure Element (SE 200) in order to inform the Secure Element (SE 200) of the successful completion of the transfer.~~

2~~3~~. Method of claim 1 ~~or 2~~, wherein the Secure Activation module (202) and the Watermark inserter (201) are located in a Trusted environment, the connection between these two elements is not accessible outside of the Trusted environment.

3~~4~~. Method of one of the claims 1 or~~to~~ 2~~3~~, wherein the CAS Data comprises a unique identifier, said identifier being transferred to the Secure Activation module (202) and to the Watermark inserter (201) together with the watermark instruction while enabling the watermarking, said identifier defining a payload to watermark the content.

4~~5~~. Client device comprising a Conditional Access Module (CAS) in charge of receiving and decrypting CAS Data to obtain a watermark instruction and a content key (CW), a Descrambler (DSC) having an input to receive an encrypted compressed content and an output to produce a decrypted compressed content based on the content key, a decoder to convert the decrypted compressed content into uncompressed content, a Watermark inserter (201) connected to the output of the Decoder to insert a watermark based on the watermark instruction, a Secure Activation module (202) connected with the Watermark inserter (201), a Secure Element (SE 200) connected with the Conditional Access Module (CAS), the Descrambler (DSC) and the Secure Activation module (202), characterized in that, the Conditional Access Module (CAS) has means to verify a signature of the CAS data and in case that the signature is valid, has means to transfer the watermark instruction to the Secure Activation module (202) via the Secure Element (SE200), said Secure Element (SE200) has means to verify that the watermark instructions was successfully transferred to the watermark inserter, and in case of successful transfer, has means to transfer the content key to the descrambler (103)~~.~~, wherein the Secure Activation module (202) comprises a random number generator able to produce a random number (X), said Secure Activation module (202) generating, storing and sending said random number to the Secure Element (SE 200) which prepares a message containing at least the watermark instruction, the random number, and a signature on both the watermark instruction and the random number, said Secure Activation module (202) having means to verify if the signature

is authentic and if the random number is the same as the one stored, in the positive event, accepting the watermark instruction and sending a final acknowledgment message to the Secure Element (SE 200) in order to inform the Secure Element (SE 200) of the successful completion of the transfer.

~~6. Client device of the claim 5, wherein the Secure Activation module (202) comprises a random number generator able to produce a random number (X), said Secure Activation module (202) generating, storing and sending said random number to the Secure Element (SE 200) which~~

~~prepares a message containing at least the watermark instruction, the random number, and a signature on both the watermark instruction and the random number, said Secure Activation module (202) having means to verify if the signature is authentic and if the random number is the same as the one stored, in the positive event, accepting the watermark instruction and sending a final acknowledgment message to the Secure Element (SE 200) in order to inform the Secure Element (SE 200) of the successful completion of the transfer.~~