

Abstract**Method for protecting decryption keys in a decoder and decoder for implementing said method**

- 5 Method for securing control words (CW) within a decoder (10) in charge of descrambling digital content protected by these control words, comprising the following steps:
- for each descrambling unit (14) of this decoder, loading in a directory (22) a pairing key (PK) referenced by an identifier (ID) associating said key to a descrambling unit,
- 10 - receiving at least one encrypted control word referenced by an indication (D) allowing to identify the descrambling unit for which it is intended,
- decrypting the control word by using a first key shared with a security module (30),
 - identifying in the directory the pairing key whose identifier (ID) corresponds to the indication of destination (D) associated to the control word,
- 15 - encrypting this control word by using this pairing key,
- storing in a register (15) the control word in a chronological and referenced way.

(Fig. 1)