Abstract

The invention relates to a data storage medium having a semiconductor chip which has at least one memory in which an operating program is stored which contains a number of commands, with each command producing signals which can be detected from outside the semiconductor chip.

According to the invention the data storage medium is designed in order to split secret data, which is stored in the semiconductor chip in order to carry out security-relevant or safety-relevant operations or is generated by this semiconductor chip, into at least three data parts, with an arithmetic unit being included in order to calculate a random number and in order to divide the random number, with the first data part being the integer result of the division process, the second part being the remainder of the division process, and the third part being the random number itself.



162162



G00002