

ABSTRACT

5 The aim of this invention is to improve in an optimal way the security of smart cards to prevent the fraudulent control of a cryptographic processor(s) by means of external signals that interfere with the normal development of the tasks of a processor(s).

10 This aim is reached by a component IC of a security module comprising at least two processors CPU A, CPU B each connected to program memories ROM A, ROM B, to non-volatile programmable and erasable memories (EEPROM) EEPROM A, EEPROM B containing the data and random access memories (RAM) RAM A, RAM B that serve as temporary data storage during processing, the first processor CPU A having an interface bus with the exterior of the component IC, characterized in that the second processor CPU B is connected to the first processor CPU A through an exchange memory DPR, the non-volatile programmable and erasable memory EEPROM A of the first processor CPU A
15 having read-only access R for said first processor CPU A, the second processor CPU B having read and write access RW on said non-volatile programmable and erasable memory EEPROM A of the first processor CPU A.