

ABSTRACT

PROCESS FOR PROTECTING A SECURITY MODULE, AND ASSOCIATED SECURITY MODULE

The invention relates to a process for protecting a security module (8) designed to cooperate with a data processing device (1), the module being designed to execute a set of operations including at least one sensitive operation (23).

According to the invention, the process includes the steps comprised of:

- executing, at the time of each execution of the sensitive operation and upstream from the latter, a first supplementary sequence of operations (22) intended to activate signaling means, and downstream from said sensitive operation, a second supplementary sequence of operations (24) intended to deactivate said signaling means;

- verifying, at the time of each execution of the sensitive operation and upstream from said first supplementary sequence of operations (22), whether the signaling means have been deactivated;

- in the case where the signaling means are activated, inhibiting the execution of the sensitive operation.

Figure 2.