

ABSTRACT

The aim of this invention is to propose a transmission method of a message containing a program block that allows to avoid the consequences of a possible malicious decryption of this message.

- 5 This aim is achieved through a secure method to update software embedded in a security module, this method comprising the following steps:
- formation of a first updating program block (PBI),
 - determination of a target memory zone of said security module,
 - determination through said security module, of a pre-registered content
 - 10 (MM_Ref) in said target memory zone ,
 - formation of a second program block (SBI) obtained by the mixing of all or a part of the pre-registered content with the first program block (PBI),
 - transmission of the second program block (SBI) to the security module,
 - reception of the second block by the security module,
 - 15 - reading of the target memory zone (MEM),
 - obtaining and writing in the target memory zone of the first block by the inverse mixing of all or part of the second block and of the target memory zone content.