ABSTRACT

The aim of this invention is to propose a method for the authentication of applications both at the time of their downloading as well as at the time of their execution.

This aim is reached by an authentication method of at least one application (APP) working in a equipment (CB) connected by a network (NET) to a control server (CSE), said equipment (CB) being locally connected to a security module (SIM), said application (APP) is loaded and/or executed by means of an application execution environment (AEE) of the equipment (CB) and uses resources (RES) stored in the security module (SIM), comprising the following preliminary steps:

- reception by the control server (CSE), via the network (NET), of data comprising at least the identifier (IMEISV) of the equipment (CB) and the identifier (IMSI) of the security module (SIM),

- analysis and verification by the control server (CSE) of said data,

- generation of a cryptogram (CRY) comprising a digest (FIN1) of the application (APP), data identifying the equipment (CB) and the security module (SIM) and instructions (INS RES) intended for said module,

- transmission of said cryptogram (CRY), via the network (NET) and the equipment (CB), to the security module (SIM),

- verification of the application (APP) by comparing the digest (FIN1) extracted from the cryptogram (CRY) received with a digest (FIN2) determined by the security module (SIM),

said method is characterized in that, during the initialization and/or the activation of the application (APP), the security module (SIM) executes the instructions (INS_RES) extracted from the cryptogram (CRY) and releases, respectively blocks the access to certain resources (RES) of said security module (SIM) according to the result of the verification suited to this application (APP) carried out previously.