CLAIMS

1. A method (30) for managing at least one processing relating to an application supported or to be supported by a token (14), the token comprising means (22) for processing data, means (24) for storing data and means (26) for communicating with outside,

characterized in that the method comprises the following steps:

- the token sends (38) data for requesting at least one token user to give her/his authorization (38) before executing the at least one processing relating to an application supported or to be supported by the token;
- the token verifies (316) whether the at least one token user gives her/his authorization; and
- if the at least one token user gives her/his authorization, then the token authorizes (318) to execute the at least one processing relating to an application supported or to be supported by the token.

2. Method according to claim 1, wherein, before a first step, the first step consisting in that the token sends (38) data for requesting at least one token user to give her/his authorization before executing the at least one processing relating to an application supported or to be supported by the token, the token generates data to send to outside, the data being relative to a pre-authorization number, the data being used to generate rights for authorizing the token to process a request for executing the at least one processing relating to an application supported or to be supported by the token.

3. Method according to claim 1 or 2, wherein, to give her/his authorization, the at least one token user enters a password, such as a Personal Identification Number, and/or personal biometric data, so as to authenticate the at least one token user.

4. Method according to any of claims 1 to 3, wherein the at least one processing relating to the application supported or to be supported comprises at least one element belonging to a group comprising:

- a downloading of the application into the means for storing data;
- a loading of the application into the means for storing data;
- a moving of the application within the means for storing data;
- an installation of the application within the means for storing data;
- an execution of the application by the means for processing data;
- a modification of the application by the means for processing data;
- a deletion of the application within the means for storing data.

5. Method according to any of claims 1 to 4, wherein, before a first step, the first step consisting in that the token sends (38) data for requesting at least one token user to give her/his authorization, the at least one token user enters an authorization number based upon data originating from a token issuer, the token issuer issuing the token.

6. Method according to any of claims 1 to 5, wherein the application supported or to be supported by the token is associated with one secure memory area of the token under one and the same control of the at least one token user, the secure memory area being included within the means for storing data.

7. Method according to any of claims 1 to 6, wherein, the token cooperating with a terminal, a first step, the first step consisting in that the token sends (38) data for requesting at least one token user to give her/his authorization before executing the at least one processing relating to an application supported or to be supported by the token, is carried out through a graphical application supported by the terminal, the graphical application being authenticated by the token.

8. Method according to any of claims 1 to 7, wherein, before a first step, the first step consisting in that the token sends (38) data for requesting at least one token user to give her/his authorization before executing the at least one

processing relating to an application to be supported by the token, the token receives data originating from outside, the data comprising a request for creating one secure memory area of the token under one and the same control of the at least one token user, one secure memory area of the token being created under one and the same control of the at least one token user and associated with an application issuer, the application issuer issuing the application to be supported by the token.

9. A token (14) for managing at least one processing relating to an application supported or to be supported by a token, the token comprising means (22) for processing data, means (24) for storing data and means (26) for communicating with outside,

characterized in that the token is adapted to:

- send (38) data for requesting to at least one token user to give her/his authorization before executing the at least one processing relating to an application supported or to be supported by the token;
- verify (316) whether the at least one token user gives her/his authorization; and
- authorize (318), if the at least one token user gives her/his authorization, to execute the at least one processing relating to an application supported or to be supported by the token.

CLAIMS

1. A method for managing at least one processing relating to an application supported or to be supported by a device, the device including a chip, the chip comprising means for processing data, means for storing data and means for communicating externally of the chip, the chip being coupled to a host device, wherein the method comprises the following steps: sending, by the chip, as a master, to the host device, a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application supported or to be supported by the chip; verifying, by the chip, whether the at least one chip user has provided an authorization; and authorizing, by the chip, only if the at least one chip user provides an authorization, a creation of a secure memory area within the chip, the secure memory area being included within the means for storing data.

2. The method according to claim 1, wherein, before a first step of sending a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application supported or to be supported by the chip, the chip generates data to send externally, the data being relative to a pre-authorization number, the data being used to generate rights for authorizing the chip to process a request for executing the at least one processing relating to an application supported or to be supported by the chip.

3. The method according to claim 1, wherein, to provide an authorization of the chip user, the at least one chip user enters a password, such as a Personal Identification Number, or personal biometric data, so as to authenticate the at least one chip user.

4. The method according to claim 1, wherein the at least one processing relating to the application supported or to be supported comprises at least one element belonging to a group comprising: a downloading of the application into the created secure memory area; a loading of the application into the created secure memory area; a moving of the application within the created secure memory area; an installation of the application within the created secure memory area; an execution of the application by the means for processing data; a modification of the application by the means for processing data; a deletion of the application within the created secure memory area.

5. The method according to claim 1, wherein, before the first step of sending a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip, the at least one chip user enters an authorization number based upon data originating from a chip issuer, the chip issuer issuing the chip.

6. The method according to claim 1, wherein the chip supports a self-issuer application, the self-issuer application generates a signature based upon the chip user authorization and sends the generated signature to the secure memory area to be created.

7. The method according to claim 1, wherein the first step of sending a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application supported or to be supported by the chip, is carried out through a page relating to a web server embedded within the chip.

8. The method according to claim 1, wherein, the host device is a terminal with which the chip cooperates, and the first step of sending a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application supported or to be supported by the chip, is carried out through a graphical application supported by the terminal, the graphical application being authenticated by the chip.

9. The method according to claim 1, wherein, before the first step of sending a proactive command for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application to be supported by the chip, the chip receives data originating externally, the data originating externally comprising a request for creating one secure memory area of the chip under one and the same control of the at least one chip user, a secure memory area of the chip being created under one and the same control of the at least one chip user and associated with an application issuer, the application issuer issuing the application to be supported by the chip.

10. A device for managing at least one processing relating to an application supported or to be supported by the device, the device including a chip, the chip being coupled to a host device, the chip comprising: means for processing data; means for storing data; and means for communicating externally of the chip, wherein the means for processing data is configured to (i) function as a master and send a proactive command to the host device for requesting at least one chip user to provide an authorization to create a secure memory area within the chip before executing the at least one processing relating to an application supported or to be supported by the chip, (ii) verify whether the at least one chip user provides an authorization; and (iii) authorize, if the at least one chip user provides an authorization, an execution of a creation of a secure memory area within the chip, the secure memory area being included within the means for storing data.

11. The device according to claim 10, wherein the secure memory area is dedicated to store an application to be imported from outside the chip.

12. The device according to claim 10, wherein the device is included within at least one element of a group comprising: a smart card; a SIM type card; a USB type dongle; a MMC card; a SD card; and an embedded secure element.

13. The device according to claim 10, wherein the host device is included within at least one element of a group comprising: a mobile telephone; a set-up box; a desktop computer; a laptop computer; a media player; a game console; a handset; a Personal Digital Assistant.