CLAIMS

1. Method for the mutual authentication of a controllable functional electronic device and of its user, the method comprising:

- a preliminary device configuration phase defining the modalities for verifying its authenticity,

- a prior authentication phase of the device by the user,

- an operational phase initiated by the user and including a preliminary step of authentication of the user by the device, the preliminary step of authentication of the user by the device comprising providing an operational question to the user, receiving a response from the user, and verifying that there is identity between the response provided by the user and an expected operational response, the user then being able to control the device to provide a determined service,

the device containing sensitive or confidential data and being arranged so as to, in the operational phase initiated by the user, execute a specific operation appropriate to provide the service,

the method comprising, before any operational phase is performed, a preliminary device authentication phase

the prior authentication phase of the device by the user being based on a question-answer authentication process, by means of a device authentication secret which is a preliminary question from the user to the device and a preliminary answer to the preliminary question from the device to the user, the preliminary question and the preliminary answer being secret so as to be known or accessible only to the sole genuine user, such that the authenticity of the device is only proven if, and only if, the user verifies that there is identity between, on the one hand, the answer provided by the device to the preliminary question and, on the other hand, the preliminary answer, such that:

- if, at the end of the preliminary device authentication phase, the device is proven to be genuine, the user can perform the operational phase,

- if, at the end of the preliminary device authentication phase, the device is not proven to be genuine, the user can prevent execution of the operational phase,

such that, first the device and then the user are authenticated, and the operation and the service provided are secure,

the method further comprising deletion, by the electronic device, of the confidential data, if the user has not provided the preliminary question during a predetermined number of executions of the preliminary device authentication phase by the user, the electronic device therefore considering that the user is not the genuine user.

2. Method according to claim 1, wherein the preliminary configuration phase configures the device with the device authentication secret.

3. Method according to claim 2, in which the preliminary configuration phase of the device is performed by the user.

4. Method according to claim 3 wherein the configuration of the device with the preliminary question and the preliminary answer is done using a question from the, through a question-to-answer generation process.

5. Method according to one of claims 2 to 4, in which the preliminary device authentication phase is executed after the preliminary configuration phase has been executed, and under the condition that no other preliminary authentication phase or operational phase of the device has been executed in the meantime.

6. Method according to one of claims 2 to 4, in which the preliminary device authentication phase is executed after the preliminary configuration phase has been executed, and under the condition that one or more other preliminary authentication phases or operational phases of the device have been executed in the meantime.

7. Method according to one of claims 2 to 4, in which a preliminary configuration phase is necessarily and sufficiently combined with either a single preliminary device authentication phase or a pre-set plurality of successive preliminary device authentication phases or an unlimited number of successive preliminary device authentication phases.

8. Method according to one of claims 1 to 7, wherein the preliminary step for the authentication of the user by the device is based on a user authentication secret which is an operational answer from the user to the device, which is secret so as to be known and accessible only to the sole genuine user, such that the authenticity of the user is proven if, and only if, the device verifies that there is equivalence between the answer provided by the user and the operational answer.

9. Functional electronic device, controllable by a user concerning a determined service, containing sensitive or confidential data, configured for the implementation of the mutual authentication method according to any one of claims 1 to 8.

10. Method according to any one of claims 1 to 8, implemented with a plurality of electronic devices forming one or more functional chains with one or more upstream devices and one or more downstream devices, in which:

- if, at the end of the prior authentication phase of an upstream device in a chain of devices, this device is proven to be genuine, the downstream device(s) in the same chain of devices are also authenticated,

- if, at the end of the preliminary authentication phase of an upstream device in a chain of devices, this device is not proven to be genuine, the downstream device(s) in the same chain of devices are not authenticated, the system being proven not to be genuine.