

Claims

1. A method for checking an integrity of an electronic device, the electronic device comprising:

- a secure element, capable of storing and managing data and onto which a public key has been loaded, and intended for verifying an electronic signature, wherein the electronic signature was initially produced during a preliminary configuration phase of the electronic device,
- a processor configured to collaborate with the secure element, and
- a means of storing data, comprising a memory whose entire content has been initially authenticated and whose integrity can be verified using the public key, the memory comprising a code executable by the processor,

wherein:

in response to a request from the processor when the device is started, the secure element performs, on the entire content of the memory of the data storage means received through the processor, an authentication check of the entire content of the memory, in order to check, using the public key, that the entire content has not been modified since the initial authentication, the device being considered to be integral by the secure element when the authentication check has been successful,

the secure element stores a reference time interval T which is configured to be less than a maximum time required for the secure element to recover, through the processor, the entire content of the memory to be authenticated,

the authentication check of the entire content of the memory includes the following successive steps performed by the secure element and repeated until the entire content of the memory has been received:

- sending to the data storage means, through the processor, a request to send one or more sequences of data extracted from the memory,

- measuring a time which elapses between sending the request and receipt of the sequence or sequences requested, and comparing the time with the reference time interval T , and

- if the elapsed time is greater than the reference time interval T , refusing to authenticate the entire content of the memory of the data storage means and interrupting execution of the subsequent steps of the authentication check.

2. The method of claim 1, in which, when the device is considered to be integral, the secure element device is able to operate according to a nominal behaviour which has been attributed to it.

3. The method of claim 1, in which when the authentication check fails, the secure element is programmed to operate in a suitable mode taking into account a failure of the authentication check.

4. The method of claim 1, wherein during the preliminary configuration phase for configuration of the electronic device, the initially authenticated entire content of the memory of the data storage means is validated using the electronic signature system using a private key corresponding to the public key loaded on the secure element.

5. The method of claim 4, in which the electronic signature initially produced during the preliminary configuration phase of the electronic device is loaded either into the data storage means, or into the memory of the secure element.

6. The method of claim 1, in which the authentication check is performed either when the device is started or when the device receives a request from a user for an integrity check.

7. The method of claim 1 wherein, a failure of the authentication check on the entire content of the memory leads to the use of one or more of the following degraded operating modes:

- a user is notified of the failure of the integrity check,
- access to the data loaded on the secure element is blocked,
- access to the electronic device is blocked,
- all or part of the data stored in the electronic device is erased.

8. The method of claim 1, in which, when the time elapsed between the sending by the secure element of a request to send one or more sequences of data extracted from the memory and the receipt of the requested sequence or sequences is less than the time interval T, the secure element verifies the integrity of the sequence or sequences received with respect to the authenticity of the entire content of the memory which it must validate.

9. The method of claim 1, wherein the processor is a microcontroller and the memory of the data storage means is a memory of the microcontroller.

10. An electronic device comprising:

- a secure element capable of storing and managing data and into which has been loaded a public key intended to verify an electronic signature, wherein the electronic signature was initially produced during a preliminary configuration phase of the electronic device,

- a processor configured to collaborate with the secure element, and

- a means of data storage comprising a memory whose entire content has been initially authenticated and whose integrity can be verified using the public key, the memory comprising a code executable by the processor,

wherein:

the secure element is configured to perform, in response to a request from the processor when the device is started, on the entire content of the memory of the data storage means received through the processor, an authentication check of the entire content of the memory, in order to check, using the public key, that the entire content has not been modified since the initial authentication, the device being considered to be integral by the secure element when the authentication check has been successful,

the secure element is configured to store a reference time interval T which is configured to be less than a maximum time required for the secure element to recover, through the processor, the entire content of the memory to be authenticated,

the secure element is configured to perform and repeat the following successive steps, until the entire content of the memory has been received:

- sending to the data storage means, through the processor, a request to send it one or more sequences of data extracted from the memory,

- measuring a time which elapses between sending the request and receipt of the sequence or sequences requested, and compares the time with the reference time interval T, and

- if the elapsed time is greater than the reference time interval T, refusing to authenticate the entire content of the memory of the data storage means and interrupting execution of the subsequent steps of the authentication check.

11. The electronic device of claim 10, in which the processor is a microcontroller and the memory of the data storage means is the memory of the microcontroller.

12. The electronic device of claim 10, including one or more of the following complementary means:

- a human/machine interface, in particular a keyboard or screen,
- a communication interface with external digital devices, in particular a computer, a communication network or a remote server.

13. The method of claim 1, wherein the electronic device takes the form of a flat box and is configured for an execution of financial transactions involving cryptocurrencies.