CLAIMS

1. A method for securely processing, within a secure element, digital information, said secure element including a secure processor adapted for security-critical applications, and at least one internal memory and a code associating unit, both external to the secure processor, wherein the method provides an end-to-end security ensuring that the digital information has not been altered from storage in an external memory to processing by the secure processor, and comprises the steps, performed by the secure element:

- loading the digital information from the external memory into the at least one internal memory of the secure element;
- decrypting the digital information to obtain the digital information in clear and a first integrity element;
- by the code associating unit, segmenting the digital information in clear into words of digital information, generating error-detection codes or error-correction codes from said words of digital information and associating said error-detection codes or error-correction codes with the corresponding words in the at least one internal memory;
- verifying the integrity of the digital information in clear by calculating an integrity element based on the segmented words and comparing the calculated integrity element with the first integrity element obtained during decryption, ensuring that the digital information has not been altered before transferring;
- transferring the words of digital information and the associated error-detection codes or error-correction codes from the at least one internal memory to the secure processor;
- by the secure processor, verifying the words of digital information based on the associated error-detection codes or error-correction codes before processing the digital information contained in said words.

2. The method according to claim 1, further including a step of verifying the integrity of the digital information in encrypted form.

3. The method according to claim 1, wherein the words of digital information are stored in an internal memory of the secure element in association with the error-detection codes or error-correction codes and, in said step of verifying the integrity of the digital information performed after the step of associating the words of digital information with the error-detection codes or error-correction codes, said words of digital information are read from the internal memory to perform the verification of integrity.

4. The method according to claim 1, wherein the words of digital information and the associated error-detection codes or error-correction codes are transferred to the secure processor only if the integrity of the digital information is successfully verified after the step of associating the associating error-detection or error-correction codes with the corresponding words.

5. The method according to claim 1, wherein the digital information is segmented into words of a predetermined size that depends on a working format of the secure processor or on a capacity of registers of the secure processor.

6. The method according to claim 1, wherein, the digital information being stored in segments in the external memory, the step of loading the digital information and the step of segmenting the digital information into words are performed iteratively for each of the segments.

7. The method according to claim 1, wherein:

- in the step of loading each segment from the external memory, the secure element loads digital information in encrypted form and an integrity element,
- in the step of verifying the integrity of the digital information in encrypted form, the secure element calculates an integrity element by chaining calculations on L+1 blocks of a predetermined number of bytes in encrypted form, and compares the calculated integrity element with the integrity element loaded.

8. The method according to claim 1, wherein

- in the step of decrypting, N+1 blocks in encrypted form are decrypted into N

blocks of digital information in clear and another integrity element;

- in the step of segmenting, each of the N blocks of digital information in clear is divided into words of digital information.

9. The method according to claim 1, wherein

- in the step of verifying the integrity of the digital information performed after the step of associating the error-detection codes or error-correction codes with the corresponding words, the secure element calculates an integrity element by chaining calculations on L blocks of digital information in clear, and compares said calculated integrity element with said other integrity element resulting from the step of decrypting.

10. The method according to claim 1, further including the following steps, performed by a digital information provider:

- segmenting the digital information in clear into segments;

- and, for each segment of digital information:

. calculating a first integrity element for the digital information in clear;

. encrypting the digital information and the first integrity element;

. calculating a second integrity element of the result of the encryption and concatenating the result of the encryption and said second integrity element;

. storing the result of the encryption concatenated with said second integrity in the external memory.

11. The method according to claim 10, wherein, when a segment of digital information has been modified by the secure element, said secure element updates said segment of digital information in the external memory by executing the steps of:

. calculating a first integrity element for the digital information in clear;

. encrypting the digital information and the first integrity element;

. calculating a second integrity element of the result of the encryption and concatenating the result of the encryption and said second integrity element;

. updating the segment currently stored in the external memory with the result of the encryption concatenated with the second integrity element.

12. The method according to claim 1, wherein the words of digital information are processed by the secure processor only if no error is detected in said words of digital information.

13. The method according to claim 1, wherein, when the step of verifying a word of digital information by the secure processor based on the associated error-detection code or error-correction code fails, said word of the digital information is handled as not relevant or the method for securely processing the digital information is aborted.

14. A non-transitory computer readable medium including program instructions for causing a secure element for securely processing digital information, said secure element having a secure processor, to perform the steps of the method according to claim 1.

15. A secure element for securely processing digital information, including:

- a secure processor adapted for security-critical applications;
- at least one internal memory;
- a communication interface for loading the digital information from an external memory into the at least one internal memory of the secure element;
- a decryption unit for decrypting the digital information to obtain the digital information in clear and a first integrity element;
- a code associating unit for segmenting the digital information in clear into words of digital information, generating error-detection codes or error-correction codes from said words of digital information and associating said error-detection codes or error-correction codes with the corresponding words in the at least one internal memory;
- an integrity verification unit for verifying the integrity of the digital information in clear by calculating an integrity element based on the segmented words and comparing the calculated integrity element with the first integrity element obtained during decryption, ensuring that the digital information has not been altered before transferring the segmented words from the at least one internal memory to the secure processor;

wherein the secure processor is configured to load the words of digital information and the associated error-detection codes or error-correction codes from the at least one internal memory and verify said words of digital information based on the associated error-detection codes or error-correction codes before processing the digital information contained in said words.

16. The secure element of claim 15, further including an integrity verification unit for verifying the integrity of the digital information in encrypted form and a decryption unit for decrypting the digital information that has been loaded to obtain the digital information in clear.

17. A system on the chip including the secure element according to claim 15.

18. The system on the chip according to claim 17, further including an external memory located outside the secure element.

19. A hardware module including the system on the chip according to claim 18.

20. The hardware module according to claim 19, wherein said external memory that is located outside the secure element is located either inside the system on the chip or outside the system on the chip.