

CLAIMS

1. A method for securely processing digital information, including the following steps, performed by a secure element (100) including a secure processor (102), and at least one internal memory (107) and a code associating unit (106), both external to the secure processor (102) :
- loading (S10) the digital information (S_i'') from an external memory (200) into the at least one internal memory (107) of the secure element (100);
 - 10 - at the code associating unit (103), segmenting (S13) the digital information (S_i) into words of digital information ($W_{i,j,k}$), generating error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{i,k}$) 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 (107);
 - 15 - transferring (S15) the words of digital information ($W_{i,j,k}$) and the associated error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) from the at least one internal memory (107) to the secure processor (102);
 - 20 - in the secure processor (102), verifying (S16) the words of digital information ($W_{i,j,k}$) based on the associated error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) before processing the digital information contained in said words ($W_{i,j,k}$).
2. The method according to claim 1, further including a step (S14) of
- 25 verifying the integrity of the digital information that is performed after the step (S13) of associating the error-detection codes or error-correction codes with the corresponding words and before transferring (S15) the words of digital information and the associated error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) to the secure processor (102).

3. The method according to any of claims 1 and 2, further including a step (S12) of decrypting the digital information loaded from the external memory (200) to obtain the digital information in clear, and wherein the step (S13) of segmenting into words is performed on the digital information in clear.
- 5 clear.
4. The method according to claim 3, further including a step (S11) of verifying the integrity of the digital information in encrypted form.
5. The method according to any of claims 2 to 4, characterized in that the words of digital information ($W_{i,j,k}$) are stored in an internal memory (106) of the secure element (100) in association with the error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) and, in said step (S14) 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 ($W_{i,j,k}$) are read from the internal memory (106) to perform the verification of integrity.
- 10 the secure element (100) in association with the error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) and, in said step (S14) 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 ($W_{i,j,k}$) are read from the internal memory (106) to perform the verification of integrity.
- 15 internal memory (106) to perform the verification of integrity.
6. The method according to any of claims 2 to 5, characterized in that the words of digital information ($W_{i,j,k}$) and the associated error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) are transferred to the secure processor (102) only if the integrity of the digital information is successfully verified after the step (S13) of associating the associating error-detection or error-correction codes with the corresponding words.
- 20 verified after the step (S13) of associating the associating error-detection or error-correction codes with the corresponding words.
7. The method according to any of claims 1 to 6, characterized in that the digital information is segmented into words ($W_{i,j,k}$) of a predetermined size that depends on a working format of the secure processor (102) or on a capacity of registers of the secure processor (102).
- 25 of registers of the secure processor (102).
8. The method according to any of claims 1 to 7, characterized in that, the digital information being stored in segments (S_i'') in the external memory (200), the step (S10) of loading the digital information and the step (S13) of segmenting the digital information into words are performed iteratively for each of the segments.
- 30 each of the segments.

9. The method according to claim 8 when dependent on claim 4, characterized in that:

- in the step (S10) of loading each segment from the external memory (200), the secure element (100) loads digital information in encrypted form and an integrity element (MAC_{i2}),
- in the step (S11) of verifying the integrity of the digital information in encrypted form, the secure element (100) calculates an integrity element by chaining calculations on $L+1$ blocks ($C_{i0}, \dots, C_{iL}$) of a predetermined number of bytes in encrypted form ($C_{i0}, \dots, C_{iL}$), and compares the calculated integrity element with the integrity element loaded (MAC_{i2}).

10. The method according to claims 3 and 9, characterized in that

- in the step of decrypting (S12), $N+1$ blocks in encrypted form ($C_{i0}, \dots, C_{iN}$) are decrypted into N blocks of digital information in clear ($P_{i0}, \dots, P_{iN-1}$) and another integrity element (MAC_{i1});
- in the step of segmenting (S13), each of the N blocks of digital information in clear ($P_{i0}, \dots, P_{iN-1}$) is divided into words of digital information ($W_{ij,k}$).

11. The method according to claims 10 and 2, characterized in that

- in the step (S14) of verifying the integrity of the digital information performed after the step (S13) of associating the error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) with the corresponding words ($W_{ij,k}$), the secure element (100) calculates an integrity element by chaining calculations on L blocks of digital information in clear ($P_{i0}, \dots, P_{iL-1}$), and compares said calculated integrity element with said other integrity element (MAC_{i1}) resulting from the step of decrypting (S12).

12. The method according to any of claims 1 to 11, further including the following steps, performed by a digital information provider :

- segmenting the digital information in clear into segments (S_i);
- and, for each segment of digital information (S_i):
 - . calculating a first integrity element (MAC_{i1}) for the digital information in clear;

- . encrypting the digital information and the first integrity element (MAC_{i_1}) ;
- . calculating a second integrity element (MAC_{i_2}) of the result of the encryption and concatenating the result of the encryption and said second integrity element (MAC_{i_2});
- 5 . storing the result of the encryption concatenated with said second integrity in the external memory (200).

13. The method according to claim 12, characterized in that, when a segment of digital information (Si_c) has been modified by the secure element (100), said secure element (100) updates said segment of digital information
10 in the external memory (200) by executing the steps of :

- . calculating a first integrity element ($MAC_{i_{c_1}}$) for the digital information in clear;
- . encrypting the digital information and the first integrity element ($[Si'_c] = [Si_c][MAC_{i_{c_1}}]$) ;
- 15 . calculating a second integrity element ($MAC_{i_{c_2}}$) of the result of the encryption and concatenating the result of the encryption and said second integrity element (MAC_{i_2});
- . updating the segment currently stored in the external memory (200) with the result of the encryption concatenated with the second integrity element (Si'_c)).

20 14. The method according to any of claims 1 to 13, characterized in that the words of digital information ($Wi_{j,k}$) are processed by the secure processor (102) only if no error is detected in said words of digital information.

15. The method according to any of claims 1 to 14, characterized in that, when the step (S16) of verifying a word of digital information ($Wi_{j,k}$) by the
25 secure processor (102) based on the associated error-detection code ($EDC_{j,k}$) or error-correction code ($ECC_{j,k}$) fails, said word of the digital information ($Wi_{j,k}$) is handled as not relevant or the method for securely processing the digital information is aborted.

16. A secure element (100) for securely processing digital information,
30 including:

- a secure processor (102) ;
- at least one internal memory (107);
- a communication interface (101) for loading the digital information from an external memory (200) into the at least one internal memory of the secure
- 5 element (100);
- a code associating unit (106) for segmenting the digital information into words of digital information ($W_{i,j,k}$), generating error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) from said words of digital information and associating said error-detection codes ($EDC_{j,k}$) or error-correction codes
- 10 ($ECC_{j,k}$) with the corresponding words ($W_{i,j,k}$) in the at least one internal memory (107);

wherein the secure processor (102) is configured to load the words of digital information ($W_{i,j,k}$) and the associated error-detection codes ($EDC_{j,k}$) or error-correction codes ($ECC_{j,k}$) from the at least one internal memory (107) and

15 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.

17. The secure element according to claim 16, further including an integrity verification unit (105) that is configured to verify the integrity of the digital

20 information based on the words of digital information that are read from the at least one internal memory (107).

18. The secure element of claim 16 or 17, further including an integrity verification unit (103) for verifying the integrity of the digital information in encrypted form and a decryption unit (104) for decrypting the digital

25 information that has been loaded to obtain the digital information in clear.

19. A system on the chip including the secure element according to any of claims 16 to 18.

20. The system on the chip according to claim 19, further including an external memory (200) located outside the secure element (100).

30 21. A module including the system on the chip according to claim 20.

22. The module according to claim 21, wherein said external memory (200) that is located outside the secure element (100) is located either inside the system on the chip or outside the system on the chip.

23. A non-transitory computer readable medium including program
5 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.