

Claims

1. An integrated circuitry for secure data exchange, comprising:
 - a persistent memory area (21) for storing sensitive data;
 - data transfer means for receiving sensitive data from at least one connected device, wherein said persistent memory area (21) is adapted to store the sensitive data received through said data transfer means, and wherein said data transfer means is adapted for sending the sensitive data stored in the persistent memory area (21) to the at least one connected device,
 - crypto means for de-/encrypting received/stored sensitive data based on a symmetrical crypto method using an active secure key, and

- means for initiating a generation of a new secure key after power up, to replace the active secure key.
2. A device for handling sensitive data comprising at least one first integrated circuitry (10) for forming a first trust zone and at least one second integrated circuitry (20), said second integrated circuitry (20) being in accordance with claim 1 and forming a second trust zone, wherein:
- the first integrated circuitry (10) comprises at least one secure processing unit (11) adapted for processing sensitive data, wherein the first integrated circuitry (10) is separated from the second integrated circuitry (20);
 - the persistent memory area (21) of the second integrated circuitry (20) is located within said second trust zone;
 - the processing unit (11) of the first integrated circuitry (10) is adapted to transfer the sensitive data from the first trust zone to the second trust zone for securely storing said data in the persistent memory area (21) of the second trust zone,
 - the second integrated circuitry (20) is adapted to transfer the sensitive data stored in the persistent memory area (21) to the processing unit (11) of the first trust zone,
 - wherein the first integrated circuitry (10) comprises crypto means for securely transferring the sensitive data based on the symmetrical crypto method using the active secure key which is replaceable by the said new secure key, generated by the second integrated circuitry (20) after power up.

3. The device according to claim 2, wherein the crypto means are used for securely transferring a new generated key from the second integrated circuitry (20) to the first integrated circuitry (10).
4. The device according to any of claims 2 or 3, wherein the first and second integrated circuitries (10, 20) comprise a secret one-time programmable power-on key, said power-on key being used to securely transfer from the second integrated circuitry to the first integrated circuitry (10), the said new secure key generated by the second integrated circuitry (20) after power up, wherein the one-time programmable power-on key in the second integrated circuitry (20) is preferably stored in its persistent memory area (21).
5. The device according to any of the claims 2 to 4, wherein the means for initiating a new secure key generation are adapted to initiate a new secure key generation after each transfer of sensitive data from the first integrated circuitry (10) to the second integrated circuitry (20) and/or after each transfer of sensitive data from the second integrated circuitry (20) to the first integrated circuitry (10).
6. The device according to any of the claims 2 to 5, wherein the means for initiating generation of a new secure key comprise a random number generator (23) for generating a secure key on the basis of a random number.
7. The device according to any of the claims 2 to 6, wherein the persistent memory area (21) of the second integrated circuitry (20) is a tamper-resistant non-volatile or a tamper-resistant battery back-uped memory.
8. A method for securely transferring sensitive data bidirectional between at least one processing unit (11) and an external memory device (21), which memory device (21) is adapted to store the received sensitive data, wherein an active secure key is used to de-/encrypt received sensitive data or sensitive data to

be sent at the processing unit (11) and at the external memory, and wherein the external memory device (21) initiates and generates a new secure key after power up, in order to replace the active secure key.

9. The method according to claim 8, wherein the key exchange of the new generated key from the memory device (21) to the processing unit is de-/encrypted by the active secure key.
10. The method according to any of the claims 8 or 9, wherein a secret one-time programmable power-on key is used as an initial secure key for en-/decrypting a first key exchange from the memory device (21) to the processing unit (11) after power up.
11. The method according to any of the claims 8 to 10, wherein a key generation and/or key exchange is initiated by the memory device after each data transfer of sensitive data from the processing unit to the memory device and/or from the memory device to the processing unit.
12. The method according to any of the claims 8 to 11 capable for being executed by the device according to claims 2 to 7.
13. A gambling machine comprising a device according to any of claims 2 to 7 which is capable to perform the method according to any of claims 8 to 12.
14. The gambling machine according to claim 13, wherein the processing unit (11) of the first integrated circuitry (10) controls the gambling machine and the sensitive data stored in the memory area (21) of the second integrated circuitry (20) include at least one transaction number which is used by the processing unit (11) to validate book keeping data, wherein preferably the processing unit (11) comprises a transaction number generator (12) for generating a transaction number after each game or an event which leads to a change of game related information.

Claims:

1. An integrated circuitry to securely exchange data with another integrated circuitry, comprising:

a persistent memory area to store sensitive data;

a data transferer to receive the sensitive data from a trust zone of the other integrated circuitry, wherein said persistent memory area is adapted to store the sensitive data received through said data transferer, and wherein said data transferer is adapted to send the sensitive data stored in the persistent memory area to the trust zone of the other integrated circuitry;

a cryptographic engine to decrypt the sensitive data received from the other integrated circuitry and encrypt the sensitive data to be sent and stored in the persistent memory area based on a symmetrical crypto method using an active secure key;

wherein the integrated circuitry is separated from the other integrated circuitry, and

wherein a trust zone separate from the trust zone of the other integrated circuitry is formed by the integrated circuitry, the said trust zone of the integrated circuitry comprising a key generator to generate a new secure key after power up in order to replace the active secure key.

2. A device to handle sensitive data comprising at least one first integrated circuitry to form a first trust zone and at least one second integrated circuitry to form a second trust zone, wherein the second integrated circuitry comprises:

a persistent memory area located within said second trust zone to store the sensitive data;

a second data transferer to receive sensitive data from the at least one first integrated circuitry, wherein said persistent memory area is adapted to store the sensitive data received through said second data transferer, and wherein said second data transferer is adapted to send the sensitive data stored in the persistent memory area to the at least one first integrated circuitry;

a second cryptographic engine to decrypt the sensitive data received from the at least one first integrated circuitry and encrypt the sensitive data stored in the persistent memory area based on a symmetrical crypto method using an active secure key; and

second key generator to initiate a generation of a new secure key after power up to replace the active secure key,

wherein the first integrated circuitry comprises at least one secure processing unit adapted to process the sensitive data, wherein the first integrated circuitry is separated from the second integrated circuitry,

and wherein the secure processing unit of the first integrated circuitry is adapted to transfer the sensitive data from the first trust zone to the second trust zone to securely store said sensitive data in the persistent memory area of the second trust zone,

and wherein the second integrated circuitry is adapted to transfer the sensitive data stored in the persistent memory area to the secure processing unit of the first trust zone, and

wherein the first integrated circuitry comprises a first cryptographic engine to securely transfer the sensitive data based on the symmetrical crypto method using the active secure key which is replaceable by the new secure key generated by the second integrated circuitry after power up.

3. The device according to claim 2, wherein the second cryptographic engine is used to securely transfer a new generated key from the second integrated circuitry to the first integrated circuitry.

4. The device according to claim 2, wherein the first and second integrated circuitries comprise a secret one-time programmable power-on key, said power-on key being used to securely transfer, from the second integrated circuitry to the first integrated circuitry, the said new secure key generated by the second integrated circuitry after power up, wherein the one-time programmable power-on key in the second integrated circuitry is stored in the persistent memory area of the second integrated circuitry.

5. The device according to claim 2, wherein the first integrated circuitry comprises a first key generator.

6. The device according to claim 2, wherein the second key generator is adapted to initiate a new secure key generation after each transfer of the sensitive data from at least one of the first integrated circuitry to the second integrated circuitry and/or after each transfer of the sensitive data from the second integrated circuitry to the first integrated circuitry.

7. The device according to claim 2, wherein the second key generator of the second integrated circuitry comprises a random number generator to generate a secure key on the basis of a random number.

8. The device according to claim 2, wherein the persistent memory area of the second integrated circuitry is a tamper-resistant non-volatile or a tamper-resistant battery back-uped memory.

9. A method to securely transfer sensitive data bidirectionally between at least one first integrated circuitry and at least one second integrated circuitry,

wherein the first integrated circuitry is separated from the second integrated circuitry,

wherein at least one processing unit of the first integrated circuitry is adapted to process the sensitive data and to transfer the sensitive data from a first trust zone of the first integrated circuitry to a trust zone of the second integrated circuitry separate from the first trust zone,

wherein the second integrated circuitry is adapted to transfer the sensitive data stored in the persistent memory device of the second integrated circuitry to the at least one processing unit of the first integrated circuitry,

wherein the first integrated circuitry comprises a first cryptographic engine to securely transfer the sensitive data based on a symmetrical crypto method

using an active secure key which is replaceable by a new secure key, the method comprising:

storing the sensitive data received from at least one processing unit of the first integrated circuitry to a persistent memory device of the second integrated circuitry, wherein the persistent memory device is adapted to store the sensitive data received through a data transferer of the second integrated circuitry;

decrypting, by a cryptographic engine of the second integrated circuitry, the sensitive data received from the at least one processing unit of the first integrated circuitry using an active secure key;

encrypting, by the cryptographic engine of the second integrated circuitry, the sensitive data to be sent and being stored in the persistent memory device of the second integrated circuitry using the active secure key; and

generating, by a key generator of the second integrated circuitry, a new secure key after power up and replacing the active secure key by the new secure key.

10. The method according to claim 9, further comprising decrypting and encrypting a key exchange of the new secure key from the persistent memory device to the at least one processing unit using the active secure key.

11. The method according to claim 9, further comprising decrypting and encrypting a key exchange from the persistent memory device to the at least one processing unit after power up using a secret one-time programmable power-on key used as an initial secure key.

12. The method according to claim 9, further comprising generating the new secure key or initiating a key exchange using the persistent memory device after each data transfer of the sensitive data from the at least one processing unit to the persistent memory device and/or from the persistent memory device to the at least one processing unit.

13 . A gambling machine, comprising at least one first integrated circuitry to form a first trust zone and at least one second integrated circuitry to form a second trust zone, said second integrated circuitry comprising:

a persistent memory area located within said second trust zone to store the sensitive data;

a second data transferer to receive sensitive data from the at least one first integrated circuitry, wherein said persistent memory area is adapted to store the sensitive data received through said second data transferer, and wherein said second data transferer is adapted to send the sensitive data stored in the persistent memory area to the at least one first integrated circuitry;

a second cryptographic engine to decrypt the sensitive data received from the at least one first integrated circuitry and encrypt the sensitive data stored in the persistent memory area based on a symmetrical crypto method using an active secure key; and

a second key generator to initiate a generation of a new secure key after power up to replace the active secure key; wherein

the first integrated circuitry comprises at least one secure processing unit adapted to process the sensitive data, wherein the first integrated circuitry is separated from the second integrated circuitry;

the processing unit of the first integrated circuitry is adapted to transfer the sensitive data from the first trust zone to the second trust zone to securely store said sensitive data in the persistent memory area of the second trust zone;

the second integrated circuitry is adapted to transfer the sensitive data stored in the persistent memory area to the processing unit of the first trust zone;
and

wherein the first integrated circuitry comprises a first cryptographic engine to securely transfer the sensitive data based on the symmetrical crypto method using the active secure key which is replaceable by the new secure key generated by the second integrated circuitry after power up.

14. The gambling machine according to claim 13, wherein the processing unit of the first integrated circuitry is configured to control the gambling machine, and the sensitive data stored in the persistent memory area of the second integrated circuitry include at least one transaction number which is used by the processing unit to validate book keeping data, wherein the processing unit comprises a transaction number generator for generating a transaction number after each game or an event which leads to a change of game related information.