CLAIMS

1. A computer implemented method for providing communication between a secured client computer and a remote computer, comprising:

(a) providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type;

the method further comprising with respect to each peripheral component of said components, by said processor:

(b) establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; and

(c) coding data that is communicated between the authorized remote computer and the peripheral component through said secured communication channel, said coded data being indecryptable by the processors of other of said peripheral components;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

2. The method according to claim 1, wherein said stage (b) further includes:

i. authenticating the remote computer using a non-symmetric key that includes a public key of the remote computer;

ii. authenticating the peripheral component using a non-symmetric key that includes a private key known to the peripheral component;

iii. establishing a communication key known to the authenticated remote computer and the authenticated peripheral component, the communication key being usable for the data coding between the client computer and the remote computer.

3. The method according to claim 1, wherein said coding data for communicating through said secured communication channel includes:

iv. encrypting data for transmission through said secured communication channel; or

v. decrypting data received through said secured communication channel.

4. The method according to claim 1, wherein said client computer is devoid of a processor module that is separated from any of said at

least two peripheral components and wherein the communication between said client computer and remote computer is achieved by means of said at least two peripheral components.

5. The method according to claim 1, wherein said client computer further includes processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components; and wherein said stage (b) further includes:

establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer.

6. The method according to claim 5, wherein said stage (c), further comprises:

Cl coding said data giving rise to coded data;

C2 transmitting said coded data to the processor module through said secured communication channel; and

for transmitting said coded data from the processor module to the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module that is susceptible to being compromised, thereby achieving secured communication between the peripheral component and authenticated remote computer irrespective of the utilization of said processor module.

7. The method according to claim 1 , wherein for at least one group of said peripheral components, said processor is capable of translating data of a first data type associated with one module of said group to data of a second non compatible type of the other module of said group; the method further comprising:

d) establishing a secured peer to peer communication channel with other peripheral component of said group of peripheral components;

e) coding data for communicating between the one peripheral component through said secured communication channel with said other peripheral component; said coded data is indecryptable by other of said peripheral components apart from said group; and

f) translating data of said first type to a data of said second type or vice versa, thereby facilitating communication between said group of peripheral components in a common data type.

8. The method according to claim 1, wherein said remote computer resides in the cloud.

9. A computer implemented method for providing a communication between a secured client computer and a remote computer comprising:

a. providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is

not compatible with peripheral component data types processed by processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; said client computer further includes a processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components; the method further comprising with respect to each peripheral component of said modules;

b. establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; said establishing secured communication channel includes establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

c. establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer-to-peer communication channel is established between the processor module and the remote computer;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

10. The method according to claim 9, further comprising:

d. coding data giving rise to coded data;

e. transmitting said coded data to the processor module through said secured communication channel; and

for transmitting said coded data from the processor module to the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module that is susceptible to being compromised, thereby achieving secured communication between the client computer and authenticated remote computer, irrespective of the utilization of said processor module that is susceptible of being compromised.

11. The method according to claim 9, further comprising:

f. receiving by the processor module coded data transmitted. by the authorized remote computer through said secured processor/remote computer communication channel; said coded data is not decryptable by said processor module,

g. receiving said coded data by the peripheral component through a corresponding secured communication channel,

and processor of said peripheral component,

h. decrypting said coded data,

thereby achieving secured communication between the peripheral component and authorized remote computer, irrespective of the utilization of the processor module, irrespective of the utilization of said processor module that is susceptible of being compromised.

12. A computer implemented system for providing communication between a secured client computer and a remote computer,

comprising:

a client computer that includes at least two peripheral components;

each peripheral component is configured, by a processor, to process a

corresponding peripheral component data of a data type that is not compatible

with peripheral component data types processed by a processor of other of

said at least two peripheral components; the processor of each peripheral

component is further configured to code the corresponding data of said data

type; each peripheral component of said components, by said processor is configured:

to establishe a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; and

to code data that is communicated between the authorized remote computer and the peripheral component

through said secured communication channel , said coded data is indecryptable by the processor other of said peripheral

components;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

13. The system according to claim 12, wherein said client computer is devoid of

a processor module that is separated from any of said at least two peripheral

components and wherein the communication between said client computer and

remote computer is achieved by means of said at least two peripheral components.

14. The system according to claim 12, wherein the processor of said authenticated remote computer is configured to receive, from a first authenticated peripheral component of said components and through a corresponding first trusted channel, a coded data of a first data type, decoding it using a first communication key associated with said first peripheral component and translating it to a processable data; said processor is further configured to translate processable data to data of a second data type, code it with a second communication key associated with a second authenticated peripheral component and transmit it through a corresponding second trusted channel to said. second authenticated peripheral component.

15. The system according to any one of claim 12, wherein said remote computer resides in the cloud.

16. A computer implemented system for providing a communication between a secured client computer and a remote computer comprising:

a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; said client computer further includes a processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components;

each peripheral component of said components, by said processor is configured :

to establish a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer, including establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

to establish a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer to peer communication channel is established between the processor module and the remote computer;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

17. A non-transitory computer-readable memory tangibly embodying a program of instructions executable by the computer for executing a computer implemented method for providing communication between a secured client computer and a remote computer, comprising

(a) providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by a processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type;

the method further comprising with respect to each peripheral component of said components, by said processor:

(b) establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; and

(c) coding data that is communicated between the authorized remote computer and the peripheral component through said secured communication channel, said coded data being indecryptable by the processors of other of said peripheral components;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.

18. A non-transitory computer-readable memory tangibly embodying a program

of instructions executable by the computer for executing

a computer implemented method for providing a communication between a secured client computer and a remote computer comprising:

a. providing a client computer that includes at least two peripheral components; each peripheral component is configured, by a processor, to process a corresponding peripheral component data of a data type that is not compatible with peripheral component data types processed by processor of other of said at least two peripheral components; the processor of each peripheral component is further configured to code the corresponding data of said data type; said client computer further includes a processor module that is susceptible of being compromised and further being separated from any of said at least two peripheral components; the method further comprising with respect to each peripheral component of said modules:

b. establishing a secured peer-to-peer communication channel between the peripheral component and the remote computer that is authorized to communicate with said client computer; said establishing secured communication channel includes establishing a communication key known to the remote computer and the peripheral component, the communication key is usable for the data coding between the peripheral component and the remote component;

c. establishing a secured peer-to-peer communication channel between the peripheral component and the processor module; and wherein a secured processor/remote computer peer-to-peer communication channel is established between the processor module and the remote computer;

wherein two of said at least two peripherals are keyboard and display respectively, and wherein the processor in said keyboard is configured to process corresponding data of keystrokes data type and the processor in said display is configured to process corresponding data of display data type.