What is claimed is :

1. A method comprising:

storing a first portion of an application in a computer memory of an electronic device, wherein the application further includes a second portion required for execution of the application;

storing the second portion of the application in a secure isolated region of the computer memory of the electronic device, the second portion of the application including an encrypted portion and a plaintext portion, wherein the encrypted portion prevents the first portion and the second portion of the application from functioning correctly until the encrypted portion is accurately decrypted;

establishing, using the plaintext portion, a secure encrypted communication channel with a server;

sending, using the secure encrypted communication channel, data to the server;

based at least in part on sending the data, receiving, using the secure encrypted communication channel, a decryption key from the server; decrypting the encrypted portion using the decryption key; and

executing the first portion of the application from the computer memory of the electronic and both of the encrypted portion and the plaintext portion of the second portion of the application from the secure isolated region of the computer memory in response to decrypting the encrypted portion.

2. The method of claim 1, wherein the data includes attestation information that allows the server to verify that the electronic device includes a trusted central processing unit (CPU) chip and the secure isolated region.

3. The method of claim 2 recites, wherein the attestation information includes at least one of an identifier for the CPU chip, proof that the code on the electronic device is indeed running on a device that supports hardware based secure isolation technology, or a digest of the secure isolated region.

4. The method of claim 1 recites, further comprising:

generating, using the secure isolated region, a sealing key; and

encrypting the decryption key using the sealing key.

5. The method of claim 4 recites, further comprising storing the encrypted decryption key in non-volatile memory.

6. The method of claim 1 recites, wherein the plaintext portion includes licensing code for retrieving the decryption key from the server.

7. The method of claim 1 recites, wherein the encrypted portion includes code that is critical to usage of the application.

8. The method of claim 1 recites, further comprising receiving instructions from the server, the instructions causing the secure isolated region to periodically communicate with the server in order to determine whether the secure isolated region should terminate.

9. The method of claim 1, wherein the first portion of the application calls the second portion of the application within the secure isolated region during execution of the first portion of the application from the computer memory of the electronic device and both of the encrypted portion and the plaintext portion of the second portion of the application from the secure isolated region of the computer memory.

10. An electronic device comprising:

at least one processor;

a memory storing:

a first portion of an application wherein the application further includes a second portion required for execution of the application; and

the second portion of the application in a secure isolated region of the memory, the second portion including an encrypted portion for securing the application from extraction and a plaintext portion for opening a communication channel with a server, wherein the encrypted portion prevents the first portion and the second portion of the application from functioning correctly until the encrypted portion is accurately decrypted,

the plaintext portion including computer-readable instructions that, when executed by the at least one processor, cause the at least one processor to:

establish the communication channel with the server;

receive a decryption key associated with the application from the server via the communication channel;

decrypt the encrypted portion using the decryption key; and

execute the first portion of the application from the computer memory of the electronic device and both of the encrypted portion and the plaintext portion of the second portion of the application from the secure isolated region of the computer memory in response to decrypting the encrypted portion.

11. The device of claim 10, wherein the secure isolated region includes computer-readable instructions that, when executed by the at least one processor, cause the at least one processor to send data to the server via the communication channel, the data including attestation information that allows the server to verify that the electronic device includes secure isolated technology.

12. The device of claim 11 recites, wherein the attestation information includes at least one of an identifier for the at least one processor, proof that code on the electronic device is indeed running on a device that supports hardware based secure isolation technology, and a digest of the secure isolated region.

13. The device of claim10 recites, the computer-readable instructions, when executed by the at least one processor, further cause the at least one processor to encrypt the decryption key using a sealing key generated by the secure isolated region.

14. The device of claim 13 recites, the computer-readable instructions, when executed by the at least one processor, further cause the at least one process to store the encrypted decryption key in non-volatile memory.

15. The device of claim 10 recites, the computer-readable instructions, when executed by the at least one processor, further cause the at least one processor to :

receive instructions from the server via the communication channel, the instructions including a time interval for communicating with the server; and

based at least in part on the time interval, communicate with the server to determine that a license for the application is still valid.