

CLAIMS

1. A method comprising:
 - storing a first portion of an application in a computer memory of an electronic device;
 - storing a 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;
 - 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; and
 - decrypting the encrypted portion using the decryption key.
2. A method as claim 1 recites, 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. A method as 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. A method as any of claims 1-3 recites, further comprising executing the application using the first portion of the application, the plaintext portion of the second portion, and the decrypted portion of the second portion.
5. A method as any of claims 1-4 recites, further comprising:
 - generating, using the secure isolated region, a sealing key; and
 - encrypting the decryption key using the sealing key.
6. A method as claim 5 recites, further comprising storing the encrypted decryption key in non-volatile memory.
7. A method as any of claims 1-6 recites, wherein the plaintext portion includes licensing code for retrieving the decryption key from the server.
8. An electronic device comprising:
 - at least one processor;
 - a memory storing:
 - a first portion of an application; and

a 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,

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; and

decrypt the encrypted portion using the decryption key.

9. A device as claim 8 recites, 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.

10. A device as claim 9 recites, wherein the attestation information includes at least one of an identifier for the 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.

11. A device as any of claims 8-10 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.

12. A device as claim 11 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.

13. A system comprising:

one or more processors; and

a memory storing computer-executable instructions that, when executed by the one or more processors, cause the one or more processors to:

receive data from an electronic device, the data including at least an identifier of a central processing unit (CPU) chip of the electronic device, proof that code on the electronic device is indeed running on a device that supports hardware based secure isolation technology. and a digest of a secure isolated region;

determine, using the proof that the code on the electronic device is indeed running on a device that supports hardware based secure isolation technology, that the electronic device is configured to run secure isolated technology;

determine, using the digest of the secure isolated region, that the secure isolated region of the electronic device includes at least a portion of an application; and

send a decryption key to the electronic device.

14. A system as claim 13 recites, the computer-readable instructions, when executed by the one or more processors, further cause the one or more processor to determine that the electronic device has a license to execute the application.

15. A system as claim 13 or claim 14 recites, wherein the digest of the secure isolated region includes a plaintext portion of the application and an encrypted portion of the application.