CLAIMS

1. A computer-implemented method, comprising:

configuring, by a secure interface control, communicatively coupled to a hypervisor and a hardware security module, the hardware security module for exclusive use by a secure guest managed by the hypervisor, the configuring comprising:

obtaining, by the secure interface control, a configuration request to configure the hardware security module, from a given guest of one or more guests managed by the hypervisor, via the hypervisor;

obtaining, by the secure interface control, via a secure channel, independently from obtaining the configuration request, metadata of the given guest;

verifying, by the secure interface control, that the metadata of the given guest belongs to the given guest;

determining, by the secure interface control, if the hardware security module is already configured to a specific guest of the one or more guests, wherein the specific guest and the given guest comprise different guests of the one or more guests;

based on determining that the hardware security module is not configured to the specific guest, determining, by the secure interface control, that the given guest comprises the secure guest by evaluating the metadata of the given guest, wherein the metadata comprises installation metadata to start an image of the given guest;

based on determining that the given guest comprises thea secure guest, foreclosing, by the secure interface control, establishing a configuration of the hardware security module by guests other than the given guest of the one or more guests by limiting accesses by guests to the hardware security module exclusively to the given guest of the one or more guests;

logging the given guest into the hardware security module, by the secure interface control, wherein the logging into the hardware security module comprises utilizing a secret of the given guest, wherein the metadata comprises the secret, wherein the secret is cryptographically linked to the image and cannot be utilized by another image;

based on the logging into the hardware security module, obtaining, by the secure interface control, from the hardware security module, a session code; and

retaining, by the secure interface control, the session code.

2. The computer-implemented method of claim 1, wherein the retaining comprises storing an association of the session code with a NULL session code in a table of associations in the secure interface control.

3. The computer-implemented method of claim 1 or 2, wherein the metadata of the given guest is integrity protected and the secret is encrypted by a key derived using a private key owned by the secure interface control.

4. The computer-implemented method of claim 3, wherein the private key comprises a cryptographic measure of a boot image of the given guest.

5. The computer-implemented method of claim 2, further comprising:

based on the configuring, providing, by the secure interface control, to the given guest, a new session code to utilize by the given guest in requests to the hardware security module.

6. The computer-implemented method of claim 5, wherein the providing comprises:

intercepting, by the secure interface control, a hardware security module login request from the given guest, wherein the hardware security module login request comprises login data from the given guest;

generating, by the secure interface control, new login data based on the secret of the given guest;

issuing, by the secure interface control, to the hardware security module, a new hardware security module login request from the given guest, wherein the new hardware security module login request comprises the new login data;

obtaining, by the secure interface control, a session code from the hardware security module;

based on obtaining the session code from the hardware security module, generating, by the secure interface control, the new session code;

storing, by the secure interface control, an association between the session code from the hardware security module and the new session code in the table; and

transmitting, by the secure interface control, the new session code to the given guest, responsive to the login request.

7. The computer-implemented method of claim 5, further comprising:

intercepting, by the secure interface control, a request from the given guest to the hardware security module, wherein the request comprises the new session code;

obtaining, by the secure interface control, from the table, the session code from the hardware security module associated with the new session code;

updating, by the secure interface control, the request from the given guest to comprise a new request, wherein the new request comprises the session code from the hardware security module instead of the new session code; and

issuing, by the secure interface control, the new request to the hardware security module.

8. The computer-implemented method of claim 7, further comprising:

obtaining, by the secure interface control, from the hardware security module, fulfillment of the request; and

issuing, by the secure interface control, the fulfillment of the request to the given guest.

9. The computer-implemented method of claim 8, wherein the request is selected from the group consisting of: a hardware security module secure key generation request, and a hardware security module logout request.

10. The computer-implemented method of claim 6, further comprising:

obtaining, by the secure interface control, from the hypervisor, an indication that the given guest has stopped;

identifying, by the secure interface control~~mponent~~, the association between the session code from the hardware security module and the new session code in the table;

generating, by the secure interface control~~mponent~~, a list of one or more sessions utilizing the session code from the hardware security module, based on the table; and

logging out the given guest, by the secure interface control~~mponent~~, from the one or more sessions.

11. The computer-implemented method of claim 1, further comprising:

obtaining, by the secure interface control, from the hypervisor, an indication that the given guest has stopped;

removing, by the secure interface control, the configuration.

12. The computer-implemented of claim 6, further comprising:

obtaining, by the secure interface control, from the hypervisor, an indication that the given guest has stopped;

identifying, by the secure interface control~~mponent~~, references to the given guest retained in the hardware security module; and

removing, by the secure interface control~~mponent~~, the references.

13. The computer-implemented method of any of claims 1 to 12, wherein the secure interface control~~mponent~~ is selected from the group consisting of: firmware, hardware, and software.

14. The computer-implemented method of any of claims 1 to 13, wherein determining that the given guest comprises the secure guest by evaluating the metadata of the given guest comprises verifying one of a presence or a type of the metadata.

15. The computer-implemented method of any of claims 1 to 14, wherein utilizing the secret of the given guest, comprises decrypting, by the secure interface control, the secret.

16. The computer-implemented method of claim 15, wherein the decrypting comprises utilizing a key computed exclusively by the secure interface control.

17. A computer program product comprising:

a computer readable storage medium readable by one or more processors and storing instructions for execution by the one or more processors for performing a method comprising:

configuring, by the one or more processors, communicatively coupled to a hypervisor and a hardware security module, the hardware security module for exclusive use by a secure guest managed by the hypervisor, the configuring comprising:

obtaining, by the one or more processors, a configuration request to configure the hardware security module, from a given guest of one or more guests managed by the hypervisor, via the hypervisor;

obtaining, by the one or more processors, via a secure channel, independently from obtaining the configuration request, metadata of the given guest;

verifying, by the one or more processors, that the metadata of the given guest belongs to the given guest;

determining, by the one or more processors, if the hardware security module is already configured to a specific guest of the one or more guests, wherein the specific guest and the given guest comprise different guests of the one or more guests;

based on determining that the hardware security module is not configured to the specific guest, determining, by the one or more processors~~secure interface control~~, that the given guest comprises the secure guest by evaluating the ~~-~~metadata of the given guest, wherein the metadata comprises installation metadata to start an image of the given guest;

based on determining that the given guest comprises the~~a~~ secure guest, foreclosing, by the one or more processors, establishing a configuration of the hardware security module by guests other than the given guest of the one or more guests by limiting accesses ~~by guests~~ to the hardware security module exclusively to the given guest of the one or more guests;

logging the given guest into the hardware security module, by the one or more processors, wherein the logging into the hardware security module comprises utilizing a secret of the given guest, wherein the metadata comprises the secret,

wherein the secret is cryptographically linked to the image and cannot be utilized by another image;

based on the logging into the hardware security module, obtaining, by the one or more processors, from the hardware security module, a session code; and

retaining, by the one or more processors, the session code.

18. The computer program product of claim 17, wherein the retaining comprises storing an association of the session code with a NULL session code in a table accessible to the one or more processors.

19. The computer program product of claim 17 or 18, wherein the metadata of the given guest is integrity protected and the secret is encrypted by a key derived using a private key owned by the secure interface control.

20. A system comprising:

a memory;

one or more processors in communication with the memory;

program instructions executable by the one or more processors via the memory to perform a method, the method comprising:

configuring, by the one or more processors, communicatively coupled to a hypervisor and a hardware security module, the hardware security module for exclusive use by a secure guest managed by the hypervisor, the configuring comprising:

obtaining, by the one or more processors, a configuration request to configure the hardware security module, from a given guest of one or more guests managed by the hypervisor, via the hypervisor;

obtaining, by the one or more processors, via a secure channel, independently from obtaining the configuration request, metadata of the given guest;

verifying, by the one or more processors, that the metadata of the given guest belongs to the given guest;

determining, by the one or more processors, if the hardware security module is already configured to a specific guest of the one or more guests, wherein the specific guest and the given guest comprise different guests of the one or more guests;

based on determining that the hardware security module is not configured to the specific guest, determining, by the one or more processors~~secure interface control~~, that the given guest comprises the secure guest by evaluating~~-~~ the metadata of the given guest, wherein the metadata comprises installation metadata to start an image of the given guest;

based on determining that the given guest comprises the~~a~~ secure guest, foreclosing, by the one or more processors, establishing a configuration of the hardware security module by guests other than the given guest of the one or more guests by limiting accesses ~~by guests~~ to the hardware security module exclusively to the given guest of the one or more guests;

logging the given guest into the hardware security module, by the one or more processors, wherein the logging into the hardware security module comprises utilizing a secret of the given guest, wherein the metadata comprises the secret, wherein the secret is cryptographically linked to the image and cannot be utilized by another image;

based on the logging into the hardware security module, obtaining, by the one or more processors, from the hardware security module, a session code; and

retaining, by the one or more processors, the session code.