CLAIMS

1. A computer program product for facilitating processing within a computing environment, the computer program product comprising:

at least one computer readable storage medium readable by at least one processing circuit and storing instructions for performing a method comprising:

reserving a security module for a secure guest of the computing environment, the security module being indicated in metadata used to start the secure guest, the metadata being cryptographically linked to a boot image of the secure guest, the reserving providing a reservation, and wherein the reserving comprises binding one or more queues used to communicate with the security module to the secure guest; and

managing the one or more queues based on one or more actions relating to the reservation.

2. The computer program product of claim 1, wherein the one or more actions comprises termination of the secure guest, and wherein the managing comprises deleting one or more pending requests from the one or more queues.

3. The computer program product of claim 1, wherein the one or more queues comprises at least one request queue, the one or more actions comprises an operation to submit a request to a request queue of the at least one request queue, and wherein the managing comprises confirming that the security module is reserved to the secure guest and permitting the operation based on confirming the security module is reserved to the secure guest and that the request was issued by the secure guest.

4. The computer program product of claim 1, wherein the one or more queues comprises at least one response queue, the one or more actions comprises an operation to fetch a response from a response queue of the at least one response queue, and wherein the managing comprises confirming that the security module is reserved to the secure guest and permitting the operation based on confirming the security module is reserved to the secure guest and that the operation to fetch was issued by the secure guest.

5. The computer program product of claim 1, wherein the one or more actions comprises losing access to the security module, and wherein the managing comprises flushing the one or more queues.

6. The computer program product of claim 5, wherein the method further comprises deleting pending requests to the security module, based on losing access to the security module.

7. The computer program product of claim 5, wherein the method further comprises deleting the reservation, based on losing access to the security module.

8. The computer program product of claim 1, wherein the method further comprises denying to send a request from the secure guest to a queue that is not reserved for the secure guest.

9. The computer program product of claim 1, wherein the method further comprises denying to pass a response to the secure guest that was fetched from a queue not reserved for the secure guest.

10. The computer program product of claim 1, wherein the method further comprises returning an error code to a guest, based on the guest attempting to access a queue that is not reserved for the guest.

11. The computer program product of claim 1, wherein the method further comprises determining whether the security module is in a list of accessible security modules included in the metadata used to start the secure guest, and wherein a process of reserving the security module continues, based on determining that the security module is in the list of accessible security modules included in the metadata.

12. The computer program product of claim 1, wherein the metadata is transmitted to a trusted component via a secure channel, the trusted component to perform the reserving.

13. The computer program product of claim 1, wherein the binding comprises including an indication of the reservation in a control block of a trusted component used in performing the reserving.

14. A computer system for facilitating processing within a computing environment, the computer system comprising:

a memory; and

a processor in communication with the memory, wherein the computer system is configured to perform a method, said method comprising:

reserving a security module for a secure guest of the computing environment, the security module being indicated in metadata to start the secure guest, the metadata being cryptographically linked to a boot image of the secure guest, the reserving providing a reservation, and wherein the reserving comprises binding one or more queues used to communicate with the security module to the secure guest; and

managing the one or more queues based on one or more actions relating to the reservation.

15. The computer system of claim 14, wherein the one or more actions comprises termination of the secure guest, and wherein the managing comprises deleting one or more pending requests from the one or more queues.

16. The computer system of claim 14, wherein the method further comprises determining whether the security module is in a list of accessible security modules included in the metadata used to start the secure guest, and wherein a process of reserving the security module continues, based on determining that the security module is in the list of accessible security modules included in the metadata.

17. The computer system of claim 14, wherein the method further comprises returning an error code to a guest, based on the guest attempting to access a queue that is not reserved for the guest.

18. A computer-implemented method of facilitating processing within a computing environment, the computer-implemented method comprising:

reserving a security module for a secure guest of the computing environment, the security module being indicated in metadata used to start the secure guest, the metadata being cryptographically linked to a boot image of the secure guest, the reserving providing a reservation, and wherein the reserving comprises binding one or more queues used to communicate with the security module to the secure guest; and

managing the one or more queues based on one or more actions relating to the reservation.

19. The computer-implemented method of claim 18, wherein the one or more actions comprises termination of the secure guest, and wherein the managing comprises deleting one or more pending requests from the one or more queues.

20. The computer-implemented method of claim 18, further comprising determining whether the security module is in a list of accessible security modules included in the metadata used to start the secure guest, and wherein a process of reserving the security module continues, based on determining that the security module is in the list of accessible security modules included in the metadata.