

request is sent via the secure communication channel to the secure partition, and wherein the encrypted device is unlocked by the secure partition without involvement of a host operating system of the system.

12. The method of claim 11, further comprising:

- 5 providing a token from the trusted remote console to the secure partition in the request, wherein the secure partition uses the token to unwrap a key used to decrypt blocks stored on the encrypted device.

13. The method of claim 11, further comprising:

- 10 providing a password for the encrypted device in the request, wherein the secure partition uses the password to unlock the encrypted device.

14. The method of claim 11, further comprising:

specifying in the request a management operation to be performed after the encrypted device is unlocked, wherein the secure partition performs the management operation after the encrypted device is unlocked.

15 ~~15. A computer implemented method comprising:~~

- authenticating first credentials of a user of a system before access is allowed to any device of a plurality of devices attached to the system;  
intercepting an event indicating attachment of a new device to the system, wherein the intercepting is performed by a secure partition of the system, and the secure  
20 partition is isolated from a host operating system of the system;  
requesting second credentials to access the new device, wherein the second credentials are requested without booting the system;  
authenticating the second credentials;  
enabling access to the new device after authenticating the second credentials; and  
25 delivering a hot plug event for the new device to the host operating system.

16. The method of claim 15, wherein

requesting the second credentials to access the new device comprises using trusted path connections to a display device to display a request for the second credentials and a user input device to receive the second credentials.

17. The method of claim 15, wherein  
enabling access to the new device comprises using a native command for the device to  
enable decryption of the new device.

18. The method of claim 15, wherein  
5 the second credentials comprise a password for the new device; and  
enabling access to the new device comprises using the password to unlock the new device.

19. The method of claim 15, wherein  
the second credentials comprise a user identifier; and  
enabling access to the new device comprises providing the user identifier to a trusted third  
10 party and enabling access to the new device if the trusted third party authenticates  
the user identifier.

20. An apparatus comprising:  
at least one processor;  
a secure partition isolated from a host operating system executing on the processor; and  
15 a memory comprising instructions for firmware executing in the secure partition to  
perform the following:  
authenticating first credentials of a user of a system before access is allowed to any  
device of a plurality of devices attached to the system;  
intercepting an event indicating attachment of a new device to the system, wherein  
20 the intercepting is performed by the secure partition;  
requesting second credentials to access the new device, wherein the second  
credentials are requested without booting the system;  
authenticating the second credentials;  
enabling access to the new device after authenticating the second credentials; and  
25 delivering a hot plug event for the new device to the host operating system.

21. A computer program product comprising:  
a computer-readable storage medium; and  
instructions in the computer-readable storage medium, wherein the instructions, when  
executed in a secure partition of a processing system, cause the secure partition to  
30 perform operations comprising:  
authenticating first credentials of a user of a system before access is allowed to any

device of a plurality of devices attached to the system;  
intercepting an event indicating attachment of a new device to the system, wherein  
the intercepting is performed by the secure partition, and the secure  
partition is isolated from a host operating system of the system;  
5 requesting second credentials to access the new device, wherein the second  
credentials are requested without booting the system;  
authenticating the second credentials;  
enabling access to the new device after authenticating the second credentials; and  
delivering a hot plug event for the new device to the host operating system.

10

22. A computer-implemented method comprising:  
identifying an auditable event being performed in a secure partition of a system, wherein  
the secure partition is isolated from a host operating system of the system;  
generating an audit event record for the auditable event; and  
15 writing the audit event record to an audit log, wherein the audit log is isolated from the  
host operating system.

23. The method of claim 22 wherein  
the audit log is a first audit log of a plurality of audit logs,  
the plurality of audit logs is accessible only from within the secure partition, and  
20 each audit log of the plurality of audit logs is isolated from the host operating system;  
and the method further comprises:  
determining whether the first audit log is available;  
sending the audit event record to a first audit subsystem associated with the first  
audit log if the first audit log is available, wherein the first audit subsystem  
25 performs writing the audit event record to the first audit log; and  
sending the audit event record to a second audit subsystem associated with a  
second audit log of the plurality of audit logs if the first audit log is not  
available, wherein the second audit subsystem performs writing the audit  
event record to the second audit log.

30 24. A computer-implemented method comprising:  
receiving a request to service an audit log from a secure partition of a requesting system,  
wherein the secure partition is isolated from a host operating system of the

- requesting system, the audit log contains an audit event record of an auditable event performed in the secure partition, and the audit log is isolated from the host operating system of the requesting system;
- establishing a secure communication channel with the secure partition; and
- 5 servicing the audit log via the secure communication channel.