

CLAIMS

1. A system for emulating a physically attached trusted execution environment,

comprising:

5 a reception module capable of receiving trusted execution environment commands issued by a plurality of entities over a network, each trusted execution environment command being a command to operate on a security context that corresponds to an entity that issued the command;

a security processor instance configured to perform a plurality of cryptographic and
10 security processes on keys and protected data sets in response to the trusted execution environment commands received by the reception module; the security processor instance being tied to a particular entity and the particular entity's corresponding protected data sets, the security processor instance being prevented from processing execution environment commands from other entities; and

15 an account management module configured to maintain a plurality of protected accounts, wherein a particular protected account of the plurality of accounts comprises a protected data set that corresponds to ~~a~~ the particular entity assigned to the particular account and that includes a plurality of keys corresponding to the particular entity, the protected data set not being readable outside of the system, the security
20 processor instance using at least some of the plurality of keys to perform cryptographic processes in response to one or more trusted execution environment commands received from the particular entity.

2. The system of ~~E~~Claim 1, wherein the trusted execution environment commands conform to a Trusted Platform Module (TPM) communication protocol.

25 3. The system of ~~E~~Claim 1, wherein the protected data set includes at least a portion that is

non-readable except by the security processor instance.

4. The system of Claim 1, the account management module further configured to add a new protected data set to the plurality of data sets when a new entity is added to the account, ~~particular account including a plurality of data sets each~~

5 ~~corresponding to an entity associated with the particular account, the particular data set~~

~~being a first data set, the particular entity being a first entity, and the plurality of keys~~

~~being a first plurality of keys, the particular account further comprising:~~

~~a second protected data corresponding to a second entity assigned to the particular account~~

~~and that includes a second plurality of keys corresponding to the second entity, the second~~

10 ~~protected data set not being readable outside of the system, the security processor using at~~

~~least some of the second plurality of keys to perform cryptographic processes in response~~

~~to one or more trusted execution environment commands received from the second entity.~~

5. The system of Claim 1, the account management module further configured to ~~add~~

remove a ~~new~~ protected data set ~~to~~ from the plurality of data sets after a corresponding

15 entity is no longer operating, ~~when a new entity is added to the account.~~

6. The system of Claim 1, the plurality of keys including an endorsement key, ~~account~~

~~management module further configured to remove a protected data set from the plurality~~

~~of data sets after a corresponding entity is no longer operating.~~

7. The system of Claim 1,

20 ~~wherein the particular entity is a particular device or system, the account management~~

~~module further configured to detect that the particular device or system has been rebooted~~

~~and in response reset a portion of~~ the protected data set further comprising a monotonic

counter.

8. The system of Claim 1, the protected data set further comprising non volatile memory.÷

25 ~~a policy module configured to allow actions by the particular entity dependent on whether~~

~~policy is satisfied with respect to the data set.~~

9. The system of claim 1, further comprising :

a policy module configured to allow actions by the particular entity dependent on whether policy is satisfied with respect to the data set.

5 ~~A computer program product comprising one or more computer storage media having thereon computer-executable instructions that, when executed by one or more processors of the computing system, cause the computing system to instantiate the following: an account management module configured to maintain a plurality of protected accounts, wherein a particular protected account of the plurality of accounts comprises a protected~~
10 ~~data set that corresponds to a particular entity assigned to the particular account and that includes a plurality of keys corresponding to the particular entity, the protected data set not being readable outside of the particular account, a security processor using at least some of the plurality of keys and protected data sets to perform cryptographic and security processes in response to one or more trusted execution environment commands received~~
15 ~~from the particular entity.~~

10. The system of claim 1, wherein the particular entity is a particular device or system, the account management module further configured to detect that the particular device or system has been rebooted and in response reset a portion of the protected data set.
~~computer program product in accordance with Claim 9, wherein the computer-~~

20 ~~executable instructions that, when executed by the one or more processors, further causes the computing system to instantiate the following: a security processor configured to perform a plurality of cryptographic and security processes on keys in response to the trusted execution environment commands issued by a plurality of entities over a network, each trusted execution environment command being a~~
25 ~~command to operate on a security context that corresponds to an entity that issued the command.~~

11. The system of claim 10, wherein the particular entity is a particular device or system, wherein the account management module detects that the particular device or system has been rebooted using a cryptographic statement received from the particular entity.

12. The system of claim 10, wherein the reset portion comprises a platform event log register corresponding to the particular entity.

13. The system of claim 1, the particular account including a plurality of data sets each corresponding to an entity associated with the particular account, the particular data set being a first data set, the particular entity being a first entity, and the plurality of keys being a first plurality of keys, the particular account further comprising :

a second protected data corresponding to a second entity assigned to the particular account and that includes a second plurality of keys corresponding to the second entity, the second protected data set not being readable outside of the system, the security processor instance using at least some of the second plurality of keys to perform cryptographic processes in response to one or more trusted execution environment commands received from the second entity.

14. The system of claim 13, further configured to use a non-migratable key that is non-migratable from the particular account to generate a certificate that may be used by any of the plurality of entities associated with the account.

15. The system of claim 13, the particular account further comprising an account-level data set that is not specific to any of the entities associated with the account, but is general to the account itself.

16. The system of claim 15, the account-level data set immutably storing events associated with an account.

17. The system of claim 15, further comprising :

a policy module configured to allow action by any of the plurality of entities associated

with the account dependent on whether policy is satisfied with respect to the account-level data set.

18. A computer program product comprising one or more computer storage media having thereon computer-executable instructions that, when executed by one or more processors

5 of the computing system, cause the computing system to instantiate the following :-

an account management module configured to maintain a plurality of protected

accounts, wherein a particular protected account of the plurality of accounts

comprises a protected data set that corresponds to a particular entity assigned to

the particular account and that includes a plurality of keys corresponding to the

10 particular entity, the protected data set not being readable outside of the particular

account, a security processor instance using at least some of the plurality of keys

and protected data sets to perform cryptographic and security processes in response

to one or more trusted execution environment commands received from the

particular entity, the security processor instance being tied to the particular entity

15 and the particular entity's corresponding protected data sets, the security processor

instance being prevented from processing execution environment commands from

other entities.

19. The computer program product in accordance with claim 18, wherein the computer

-executable instructions that, when executed by the one or more processors, further causes

20 the computing system to instantiate the following :

the security processor instance configured to perform a plurality of cryptographic and

security processes on keys in response to the trusted execution environment

commands issued by a plurality of entities over a network, each trusted execution

environment command being a command to operate on a security context that

25 corresponds to an entity that issued the command.

20. A system for emulating a physically attached trusted execution environment, comprising :

a reception module capable of receiving trusted execution environment commands issued by a plurality of entities over a network, each trusted execution environment command being a command to operate on a security context that corresponds to an entity that issued the command, and each trusted execution environment command conform to a Trusted Platform Module (TPM) communication protocol;

a security processor instance configured to perform a plurality of cryptographic and security processes on keys and protected data sets in response to the trusted execution environment commands received by the reception module, the security processor instance being tied to the entity and the entity's corresponding protected data sets, the security processor instance being prevented from processing execution environment commands from other entities; and

an account management module configured to maintain a plurality of protected accounts, wherein a particular protected account of the plurality of accounts comprises a plurality of data sets comprising :

a first protected data set that corresponds to a first entity assigned to the particular account and that includes a first plurality of keys corresponding to the first entity,

and

a second protected data set that corresponds to a second entity assigned to the particular account and that includes a second plurality of keys corresponding to the second entity. the plurality of protected data sets not being readable outside of the system, the security processor instance using at least some of the plurality of keys for a given protected data set to perform cryptographic processes in response to one or more trusted execution

environment commands received from an entity corresponding to the given protected data set.