What is claimed is:

1. A method comprising:

creating a virtual security coprocessor in a first processing system; and

transferring the virtual security coprocessor to a second processing system for use by the second processing system.

2. A method according to claim 1, wherein the operation of creating a virtual security coprocessor in a first processing system comprises:

generating, in the first processing system, an endorsement key for the virtual security coprocessor.

3. A method according to claim 1, further comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor; and

signing the endorsement credential in the first processing system.

4. A method according to claim 1, further comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor;

signing the endorsement credential in the first processing system; and

transmitting the endorsement credential to the second processing system in connection with transmitting the virtual security coprocessor to the second processing system.

5. A method comprising:

receiving, at a first processing system, a virtual security coprocessor from a second processing system; and

after receiving the virtual security coprocessor from the second processing system, using the virtual security coprocessor to provide at least one operation from the group of operations consisting of:

providing attestation for the first processing system; and

encrypting data for the first processing system.

6. A method according to claim 5, wherein the first processing system comprises a security coprocessor implemented in hardware, the method comprising:

using the security coprocessor implemented in hardware to support the virtual security coprocessor.

7. A method according to claim 5, wherein the operation of receiving, at a first processing system, a virtual security coprocessor from a second processing system comprises:

receiving, at the first processing system, an endorsement credential created by the second processing system for the virtual security coprocessor.

8. An apparatus comprising:

a machine accessible medium; and

instructions encoded in the machine accessible medium, wherein the instructions, when executed by a first processing system, cause the first processing system to perform operations comprising:

creating a virtual security coprocessor in the first processing system; and

transferring the virtual security coprocessor to a second processing system for use by the second processing system.

9. An apparatus according to claim 8, wherein the operation of creating a virtual security coprocessor in the first processing system comprises:

generating an endorsement key for the virtual security coprocessor in the first processing system.

10. An apparatus according to claim 8, wherein the instructions cause the first processing system to perform operations comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor; and

signing the endorsement credential in the first processing system.

11. An apparatus according to claim 8, wherein the instructions cause the first processing system to perform operations comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor;

signing the endorsement credential in the first processing system; and

transmitting the endorsement credential to the second processing system in connection with transmitting the virtual security coprocessor to the second processing system.

12. An apparatus comprising:

a machine accessible medium; and

instructions encoded in the machine accessible medium, wherein the instructions, when executed by a first processing system, cause the first processing system to perform operations comprising:

receiving a virtual security coprocessor from a second processing system; and

after receiving the virtual security coprocessor from the second processing system, using the virtual security coprocessor to provide at least one operation from the group of operations consisting of:

providing attestation for the first processing system; and

encrypting data for the first processing system.

13. An apparatus according to claim 12, wherein the first processing system comprises a security coprocessor implemented in hardware, and the instructions cause the first processing system to perform operations comprising:

using the security coprocessor implemented in hardware to support the virtual security coprocessor.

14. A processing system comprising:

a processor;

a machine accessible medium communicatively coupled to the processor; and

instructions in the machine accessible medium, wherein the instructions, when executed, perform operations comprising:

creating a virtual security coprocessor in the first processing system; and

transferring the virtual security coprocessor to a second processing system for use by the second processing system.

15. A processing system according to claim 14, wherein the operation of creating a virtual security coprocessor in the first processing system comprises:

generating an endorsement key for the virtual security coprocessor in the first processing system.

16. A processing system according to claim 14, wherein the instructions perform operations comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor; and

signing the endorsement credential in the first processing system.

17. A processing system according to claim 14, wherein the instructions perform operations comprising:

generating, in the first processing system, an endorsement credential for the virtual security coprocessor;

signing the endorsement credential in the first processing system; and

transmitting the endorsement credential to the second processing system in connection with transmitting the virtual security coprocessor to the second processing system.

18. A processing system comprising:

a processor;

a machine accessible medium communicatively coupled to the processor; and

instructions in the machine accessible medium, wherein the instructions, when executed, perform operations comprising:

receiving, at the processing system, a virtual security coprocessor from a second processing system; and

after receiving the virtual security coprocessor from the second processing system, using the virtual security coprocessor to provide at least one operation from the group of operations consisting of:

providing attestation for the processing system; and

encrypting data for the processing system.

19. A processing system according to claim 18, wherein:

the processing system further comprises a security coprocessor, implemented in hardware, and communicatively coupled to the processor; and

the processing system uses the security coprocessor implemented in hardware to support the virtual security coprocessor.

20. A processing system according to claim 18, wherein:

the processing system further comprises a physical trusted platform module (TPM) communicatively coupled to the processor; and

the processing system uses the TPM to support the virtual security coprocessor.