

WHAT IS CLAIMED IS:

1. A mobile communication device comprising:

a first trusted platform module-(60);

a second trusted platform module-(62);

a processor-(24); and

a storage medium (22)-comprising instructions that cause said processor-(24) to:

establish a root of trust for a first persona-(110), the first persona-(110) comprising a first operating system-(112) and a first trusted execution environment-(114);

establish a root of trust for a second persona-(120), the second persona (120) comprising a second operating system-(122) and a second trusted execution environment-(124);

store measurements defining the root of trust for the first persona-(110) in the first trusted platform module-(60);

store measurements defining the root of trust for the second persona (120)-in the second trusted platform module-(62); and

load the first persona (110)-and the second persona (120)-using the roots of trust for the first and second personas.

2. The device in accordance with Claim 1, wherein said storage medium-(22) further comprises instructions that cause said processor-(24) to establish mutual trust between the first trusted execution environment (110)-and the second trusted execution environment (120)-such that the first persona (110)-is coupled in communication with the second persona-(120).

3. The device in accordance with Claim 2 further comprising a high assurance guard that facilitates restricting transfer of data between the first persona (110)-and the second persona (120)-when the first persona (110)-is coupled in communication with the second persona-(120).

4. The device in accordance with Claim 1, wherein said storage medium-(22) further comprises instructions that cause said processor (24)-to transfer control of the first trusted

platform module (60) to the first persona (110) and transfer control of the second trusted platform module (62) to the second persona (120) after the first and second personas have been loaded.

5. The device in accordance with Claim 4, wherein the first trusted execution environment (114) has exclusive access to the first trusted platform module (60) and the second trusted execution environment (124) has exclusive access to the second trusted platform module (62).

6. The device in accordance with Claim 1, wherein said storage medium (22) further comprises instructions that cause said processor (24) to validate an image of the first operating system (112) and the second operating system (122) against the associated roots of trust for the first persona (110) and the second persona (120) during loading.

7. The device in accordance with Claim 1, wherein said storage medium (22) further comprises instructions that cause said processor (24) execute the first persona (110) and the second persona (120) in contexts that are isolated from each other.

8. A method of operating a mobile communication device (10), said method comprising:

- establishing a root of trust for a first persona (110), the first persona (110) including a first operating system (112) and a first trusted execution environment (114);

- establishing a root of trust for a second persona (120), the second persona (120) including a second operating system (122) and a second trusted execution environment (124);

- storing measurements defining the root of trust for the first persona (110) in a first trusted platform module (60);

- storing measurements defining the root of trust for the second persona (120) in a second trusted platform module (62); and

- loading the first persona (110) and the second persona (120) using the roots of trust for the first and second personas.

9. The method in accordance with Claim 8 further comprising establishing mutual trust between the first trusted execution environment (114) and the second trusted execution

environment-~~(124)~~ such that the first persona-~~(110)~~ is coupled in communication with the second persona-~~(120)~~.

10. The method in accordance with Claim 8, wherein loading the first persona ~~(110)~~ and the second persona-~~(120)~~ comprises loading an underlying operating system with a boot loader-~~(144)~~ signed by a device manufacturer root of trust.

11. The method in accordance with Claim 8, wherein establishing the roots of trust for the first-~~(110)~~ and second-~~(120)~~ personas comprises validating an image of the first operating system ~~(112)~~ and the second operating system ~~(122)~~ against the roots of trust for the first ~~(110)~~ and second ~~(120)~~ personas during loading.

12. The method in accordance with Claim 8 further comprising transferring control of the first trusted platform module ~~(60)~~ to the first persona ~~(110)~~ and transferring control of the second trusted platform module ~~(62)~~ to the second persona ~~(120)~~ after the first and second personas have been loaded.

13. The method in accordance with Claim 8, wherein establishing a root of trust for the first and second personas comprises:

measuring software components used to establish the first ~~(110)~~ and second ~~(120)~~ persona roots of trust; and

extending the measurements into the first ~~(60)~~ and second ~~(62)~~ trusted platform modules, wherein the measurements for the first trust anchor extend into the first trusted platform module ~~(60)~~ and the measurements for the second trust anchor extend into the second trusted platform module-~~(62)~~.

14. The method in accordance with Claim 8 further comprising:

defining a security policy for the first persona ~~(110)~~ and the second persona ~~(120)~~, wherein the security policies define how the first persona-~~(110)~~ and the second ~~(120)~~ persona access physical devices on the mobile communication device-~~(10)~~; and

enforcing the security policies with a security supervisor-~~(108)~~.

15. The method in accordance with Claim 14, wherein enforcing the security policies comprises at least one of:

enabling exclusive access for one of the first persona-(110) and the second persona-(120) to at least one of the physical devices;

enabling shared access between the first persona-(110) and the second persona (120) to at least one of the physical devices; and

denying access of at least one of the physical devices to one of the first persona (110) and the second persona-(120).

16. A non-transitory computer readable medium storing computer-executable instructions thereon for operating a mobile communication device that includes a processor, a first trusted platform module, and a second trusted platform module, the computer-executable instructions cause the processor to:

establish a root of trust for a first persona, the first persona including a first operating system and a first trusted execution environment;

establish a root of trust for a second persona, the second persona including a second operating system and a second trusted execution environment;

store measurements defining the root of trust for the first persona in the first trusted platform module;

store measurements defining the root of trust for the second persona in the second trusted platform module; and

load the first persona and the second persona using the roots of trust for the first and second personas.

17. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:

establish mutual trust between the first trusted execution environment and the second trusted execution environment such that the first persona is coupled in communication with the second persona.

18. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:
load an underlying operating system with a boot loader signed by a device manufacturer root of trust.

19. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:
transfer control of the first trusted platform module to the first persona and transfer control of the second trusted platform module to the second persona after the first and second personas have been loaded.

20. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:
define a security policy for the first persona and the second persona, wherein the security policies define how the first persona and the second persona access physical devices on the mobile communication device; and
enforce the security policies with a security supervisor.