CLAIMS

1. A mobile computing device (1) having at least one processor (101) and at least one memory (102), together providing a first execution environment and a second execution environment logically isolated from the first execution environment, the mobile computing device comprising:

a first application (14) executable within the first execution environment;

a second trusted application (16) executable within the second execution environment; and

a secure communications channel between the first application and the second trusted application,

wherein the second trusted application is configured to generate one or more data items and to provide the one or more data items to the first application (14) via the secure communications channel.

2. The mobile computing device of Claim 1, wherein the second trusted application (16) is configured to receive configuration data from the first application (14) via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

3. The mobile computing device of Claim 1, wherein a first one of the one or more data items comprises an authentication code (400) for use in authenticating a process executed by the first application (14) in the first execution environment.

4. The mobile computing device of Claim 3, wherein the second trusted application (16) is configured to generate the authentication code (400) by combining a plurality of data elements (405, 415, 425), and the plurality of data elements to be combined is dependent on the type of process to be executed.

5. The mobile computing device of Claim 4, wherein at least one of the plurality of data elements (405, 415, 425) is received by the second trusted application (16) from the first application (14) via the secure communications channel.

6. The mobile computing device of Claim 4, wherein at least one of the plurality of data elements (405, 415, 425) is stored by the second trusted application (16) within the second execution environment.

7. The mobile computing device of Claim 1, wherein the first application (14) is a mobile payment application and is configured to execute a payment transaction.

8. The mobile computing device of Claim 7, wherein the payment transaction corresponds to any one of: a remote payment transaction, an NFC-enabled transaction, and a magnetic stripe transaction.

9. The mobile computing device of Claim 8, wherein the one or more data items comprise at least one of: a unique representation (425, 540) of the payment transaction, and an authentication code (400, 500) for use in authenticating the payment transaction.

10. The mobile computing device of Claim 1, further comprising a biometric sensor (10) for use in authenticating a user of the device (1).

11. A method of managing data items in a mobile computing device (1), the mobile computing device having at least one processor (101) and at least one memory (102) together providing a first execution environment and a second execution environment logically isolated from the first execution environment, the method comprising:

establishing a secure communications channel between a first application (14) in the first execution environment and a second trusted application (16) in the second execution environment;

generating one or more data items by the second trusted application (16) and providing the one or more data items to the first application (14) via the secure communications channel; and

executing the first application (14) in the first execution environment.

12. The method of Claim 11, further comprising receiving at the second trusted application (16) configuration data from the first application (14) via the secure communications channel, the configuration data comprising instructions for generating the one or more data items.

13. The method of Claim 11 , further comprising authenticating a process executed by the first application (14) in the first execution environment, and wherein a first one of the one or more data items comprises an authentication code (400) for use in authenticating the process.

14. The method of Claim 13, wherein generating the authentication code (400) comprises combining a plurality of data elements (405, 415, 425), and the plurality of data elements to be combined is dependent on the type of process to be executed.

15. The method of Claim 14, further comprising initializing the first application (14) and second trusted application (16) by receiving setup data transmitted from a remote trusted party (44) to the first application (14) and the second trusted application (16).

16. The method of Claim 15, wherein the setup data is received by the second trusted application (16) without being processed by the first application (14).

17. The method of Claim 15, wherein the setup data comprises at least one of the plurality of data elements (405, 415, 425), and initializing the second trusted application (16) further comprises storing the at least one of the plurality of data elements by the second trusted application (16) within the second execution environment.

18. The method of Claim 15, further comprising determining which ones of the plurality of data elements are to be combined to generate the authentication code (400) based on a set of instructions forming at least a part of the setup data.

19. The method of Claim 15, further comprising:

processing the setup data by the second trusted application (16); and

identifying (a) any sensitive data elements comprised within the setup data and (b) any data elements comprised within the setup data that relate only to the first application (14).

20. The method of Claim 19, further comprising:

retaining, by the second trusted application (16), the sensitive data elements within the second execution environment; and

transmitting, from the second trusted application (16) to the first application (14) via the secure communications channel, the data elements relating only to the first application.