

What is claimed is:

1. A mobile electronic device comprising:

an identifier that identifies an operating system being launched on a mobile terminal to which the mobile electronic device is connected, wherein the mobile terminal is configured to switch between launching a secured operating system and launching a non-secured operating system lower in security level than the secured operating system, and the identifier determining ~~that whether or not~~ the operating system identified is the secured ~~a prescribed~~ operating system;

a determiner that, in a case that ~~the identifier determines that~~ the operating system identified is the secured ~~prescribed~~ operating system, performs processing to determine whether or not authentication data held in the mobile electronic device is matched to authentication data held in an authentication data holding device capable of performing communication via network; and

a permitter that, in a case that the determiner determines that there is a match, permits data processing using processing data held in a processing data holding device capable of performing communication via network.

2. The mobile electronic device according to claim 1, wherein the identifier identifies the operating system of the mobile terminal that had or has an access to the mobile electronic device.

~~3. The mobile electronic device according to claim 1 or 2,
wherein the mobile terminal has a first operating system and a second operating system which is higher in security level than the first operating system, and
wherein the prescribed operating system is the second operating system.~~

34. The mobile electronic device according to ~~any one of claims 1 or 2-3~~, wherein the authentication data holding device and the processing data holding device are implemented by a device.

45. The mobile electronic device according to any one of claims 1-34,
wherein the determiner receives the authentication data sent from the
authentication data holding device and the determiner determines whether or not the
5 authentication data received is matched to the authentication data held in the mobile
electronic device.

56. The mobile electronic device according to any one of claims 1-34,
wherein the determiner transmits the authentication data held in the mobile
10 electronic device and receives information of a result of determining whether or not the
authentication data transmitted is matched to the authentication data held in the
authentication data holding device.

67. A processing method comprising:
15 identifying an operating system being launched on a mobile terminal to which
at the mobile electronic device is connected, wherein the mobile terminal is configured to
switch between launching a secured operating system and launching a non-secured
operating system lower in security level than the secured operating system;
determining ~~that whether or not~~ the identified operating system is the secured
20 ~~prescribed~~ operating system;
performing, in a case that the operating system identified was determined to be
the ~~secured~~prescribed operating system, processing to determine whether or not
authentication data held in the mobile electronic device is matched to authentication
data held in an authentication data holding device capable of performing
25 communication via network; and
permitting, in a case that the determination processing determines that there is a
match, data processing using processing data held in a processing data holding device
capable of performing communication via network.

78. The processing method according to claim 67,

wherein the determining comprises receiving the authentication data held in the authentication data holding device and determining whether or not the authentication data received is matched to the authentication data held in the mobile electronic device.

5 | 89. The processing method according to claim 67,

wherein the determining comprises transmitting the authentication data held in the mobile electronic device and receiving information of a result of determining whether or not the authentication data transmitted is matched to the authentication data held in the authentication data holding device.

10 |

910. A non-transitory computer-readable storing medium that stores a program which comprises:

15 | identifying an operating system being launched on a mobile terminal to which ~~at~~ the mobile electronic device is connected, wherein the mobile terminal is configured to switch between launching a secured operating system and launching a non-secured operating system lower in security level than the secured operating system;

determining ~~that whether or not~~ the identified operating system is the secured ~~prescribed~~ operating system;

20 | performing, in a case that the operating system identified was determined to be the ~~secured~~ ~~prescribed~~ operating system, processing to determine whether or not authentication data held in the mobile electronic device is matched to authentication data held in an authentication data holding device capable of performing communication via network; and

25 | permitting, in a case that the determination processing determines that there is a match, data processing using processing data held in a processing data holding device capable of performing communication via network.

1011. The non-transitory computer-readable storing medium according to claim 910,

wherein the determining includes receiving the authentication data held in the authentication data holding device and determining whether or not the authentication data received is matched to the authentication data held in the mobile electronic device.

5 11~~12~~. The non-transitory computer-readable storing medium according to claim 9~~10~~,

 wherein the determining includes transmitting the authentication data held in the mobile electronic device and receiving information of a result of determining whether or not the authentication data transmitted is matched to the authentication data held in the
10 authentication data holding device.