

U.S. Patent No. 9,438,572 B2 Claim Listing

No.	Limitation
[1p]	Method for establishing a device-to-device (D2D) communication session between mobile devices which are mutually connectable via a D2D communication channel and individually connectable to a mobile network, comprising:
[1a]	preloading an initiation key on each of the mobile devices, the initiation key being associated with a validity period; and on each of the mobile devices:
[1b]	verifying a validity of the initiation key based on a current time;
[1c]	requesting a further initiation key via the mobile network if no initiation key is deemed valid;
[1d]	if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure between the mobile devices over the D2D communication channel,
[1e]	the key agreement procedure resulting in the session key based on a match of the respective initiation keys used by each of the mobile devices; and
[1f]	establishing the D2D communication session over the D2D communication channel based on the session key.

2	Method according to claim 1, wherein the preloading the initiation key comprises providing the initiation key to each of the mobile devices via the mobile network when each respective mobile device is connected to the mobile network.
3	Method according to claim 1, wherein the preloading the initiation key comprises storing the initiation key in a secure storage area of each respective mobile device.
4	Method according to claim 3, wherein the secure storage area is provided by a trusted computing subsystem of each respective mobile device.
5	Method according to claim 4, wherein at least one of the group of: verifying the validity of the initiation key, and using the initiation key in performing the key agreement procedure, is performed by the trusted computing subsystem.
[6a]	Method according to claim 1, further comprising: preloading a set of initiation keys on each of the mobile devices, the set of initiation keys key being associated with a respective set of validity periods; and
[6b]	performing a key synchronization procedure between the mobile devices over the D2D communication channel for selecting a matching one of the set of initiation keys on each of the mobile devices as the initiation key.

[7a]	Method according to claim 6, further comprising: preloading a set of key identifiers on each of the mobile devices, each of the set of key identifiers identifying a respective one of the set of initiation keys; and
[7b]	performing the key synchronization procedure based on an exchange of one or more of the set of key identifiers between the mobile devices.
8	Method according to claim 6, further comprising disabling or removing the initiation key from the set of initiation keys after use in establishing the D2D communication session.
9	Method according to claim 6, wherein the set of validity periods is constituted at least in part by different but overlapping validity periods.
10	Method according to claim 1, wherein the initiation key is associated with a virtual network identity, and wherein the verifying the validity of the initiation key further comprises determining a match of the virtual network identity on each of the mobile devices via the D2D communication channel.
11	Method according to claim 1, wherein the initiation key is associated with a usage count for limiting a number of uses of the initiation key, and wherein the verifying the validity of the initiation key is further based on the usage count.

12	Method according to claim 11, further comprising adjusting the usage count after use of the initiation key in establishing the D2D communication session.
13	Method according to claim 1, further comprising requesting a further initiation key via the mobile network if the key agreement procedure fails in providing the session key.
14	Method according to claim 1, wherein the key agreement procedure comprises: a three-pass authentication procedure; or a use of the initiation key to encrypt a message exchange between the mobile devices for obtaining a shared secret, and a Diffie-Hellman key exchange procedure which is initiated based on the shared secret.
[15p]	A non-transitory computer-readable medium configured to store instructions for, upon execution of the instructions on a mobile device, causing the mobile device to establish a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, by:
[15a]	storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period;

[15b]	verifying a validity of the initiation key based on a current time;
[15c]	requesting a further initiation key via the mobile network if no initiation key is deemed valid;
[15d]	if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and
[15e]	establishing the D2D communication session over the D2D communication channel based on the session key.
[16p]	Mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to a mobile network, the mobile device comprising:
[16a]	a storage area for storing an initiation key which is provided during a preloading procedure, the initiation key being associated with a validity period; and
[16b]	a computing subsystem for:

[16c]	verifying a validity of the initiation key based on a current time;
[16d]	requesting a further initiation key via the mobile network if no initiation key is deemed valid;
[16e]	if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and
[16f]	a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.
[17p]	Mobile network arranged for preloading an initiation key on a mobile device when the mobile device is connected to the mobile network, the initiation key being associated with a validity period, the mobile device for establishing a device-to-device (D2D) communication session with a further mobile device, the mobile device and the further mobile device being mutually connectable via a D2D communication channel and individually connectable to the mobile network, the mobile device comprising:
[17a]	a computing subsystem for:

[17b]	verifying a validity of the initiation key based on a current time;
[17c]	requesting a further initiation key via the mobile network if no initiation key is deemed valid;
[17d]	if the initiation key is deemed valid, generating a session key using the initiation key by using the initiation key in performing a key agreement procedure with the further mobile device over the D2D communication channel, the key agreement procedure resulting in the session key if the initiation key used by the mobile device matches an initiation key used by the further mobile device; and
[17e]	a mobile subsystem for establishing the D2D communication session over the D2D communication channel based on the session key.