CLAIMS:

1. A device, wherein the device comprises a non-transitory memory having processor-executable instructions stored thereon, a processor coupled to the non-transitory memory, the processor-executable instructions when executed cause the processor to:

transmit a request for an authentication key of a user of a vehicle to a third device, wherein the request for the authentication key comprises an identification (ID) of the user (id_O);

receive an authentication key (K_{id_O}) from the third device; wherein the authentication key (K_{id_O}) is used to access the vehicle by the user; and

generate a delegated authentication key (K_{id_U}) to a delegated user based on the authentication key (K_{id_O}) and an ID of the delegated user in response to receiving a request for a delegated authentication key from a second device, the request for delegated authentication key comprising the ID of the delegated user; wherein the delegated authentication key (K_{id_U}) is used to access the vehicle; wherein

$K_{id_O} = h(K, id_{Car}, id_O)$, where $h(.)$ is a cryptographic hash function, id_{Car} is an ID of the third device, and the device is configured to store the K_{id_O} in a secured memory.

2. The device according to claim 1, wherein the processor is further configured to:

generate and transmit a request to generate a new secret key;

receive an authentication request from the third device; and

transmit a superuser password, provided by the user, to the third device.

3. The device according to claim 1, wherein the processor is further configured to:

receive the ID of the third device and a random number (r), from the third device;

compute a Message Authentication Code (MAC) represented by vd using a MAC generation function with input parameters K_{id_O} and r as $vd = \text{MAC}(K_{id_O}, r)$; and

transmit an access request containing parameters $[0, id_O, vd]$ to the third device where 0 denotes a requested access is from the user of the vehicle.

4. The device according to claim 3, wherein the processor is further configured to:

receive a new authentication key (K'_{id_O}) from the third device;

update the authentication key (K'_{id_O}) in memory with the new authentication key (K'_{id_O}).

5. The device according to claim 1 wherein the processor is further configured to:

receive the ID of the second device (id_U),

determine an access policy ($\mathbf{P}_U$); and

generate the delegated authentication key (K_{id_U}), where K_{id_U} = h(K_{id_O}, id_U, $\mathbf{P}_U$), wherein h(.) is the cryptographic hash function;

store the K_{id_U} in the secured memory; and

transmit the delegated authentication key (K_{id_U}) to the second device.

6. The device according to claim 5, wherein the access policy ($\mathbf{P}_U$) include one or more of validity period, speed limit, and mileage limit.

7. The device according to claim 1, wherein the processor is further configured to:

update a blacklist in the third device.

8. The device according to claim 7, wherein updating the blacklist in the third device comprises:

generating a revoke request containing the ID of user to be revoked; and

transmitting the revoke request to the third device.

9 A method for a vehicle access authentication framework having a first device operated by a car owner, a second device operated by a delegated user, and a third device residing in a vehicle; the method which is applied to the first device comprising:

transmitting a request for an authentication key of a user of a vehicle to the third device, the request for the authentication key comprising an identification (ID) of the user (id_O);

receiving an authentication key (K_{id_O}) from the third device; wherein the authentication key (K_{id_O}) is used to access the vehicle by the user; and

generating a delegated authentication key (K_{id_U}) to a delegated user based on the authentication key K_{id_O} and an ID of the delegated user in response to receiving a request for a

delegated authentication key from the second device, the request for the delegated authentication key comprising the ID of the delegated user; wherein the delegated authentication key (K_{id_U}) is used to access the vehicle; wherein $K_{id_O} = h(K, id_{Car}, id_O)$, where $h(.)$ is a cryptographic hash function, id_{Car} is an ID of the third device, and the first device is configured to store the K_{id_O} in a secured memory.

10. The method according to claim 9, further comprising:

generating and transmitting a request to generate a new secret key;

receiving an authentication request from the third device; and

transmitting a superuser password, provided by the user, to the third device.

11. The method according to claim 9, further comprising:

receiving the ID of the third device and a random number (r), from the third device;

computing a Message Authentication Code (MAC) represented by vd using a MAC generation function with input parameters K_{id_O} and r as $vd = \text{MAC}(K_{id_O}, r)$; and

transmitting an access request containing parameters $[0, id_O, vd]$ to the third device where 0 denotes a requested access is from the user of the vehicle.

12. The method according to claim 11, further comprising:

receiving a new authentication key (K'_{id_O}) from the third device;

updating the authentication key (K'_{id_O}) in a memory of the first device with the new authentication key (K'_{id_O}).