CLAIMS

1. Method of key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes (A, B, C, D, E, F, G) and RSU nodes (R1, R2, R3), wherein said RSU nodes have a permanent connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein said method comprises the steps of:

- each vehicle node, on entering said specific geographic region, requests a set of keys from an RSU node that is within range and within that region, either

  by direct communication, or

  by through multi-hop communication,

  wherein said vehicle node sends a key request to said RSU node, said request including the vehicle node public key;
- said RSU node sends said vehicle node a set of private keys, selected from a pool of private keys available to the RSU node, said set of keys being encrypted with the vehicle node public key, wherein said set of private keys also includes a key identifier for each private key in said set;

  characterised in that it further comprises the steps of
- said RSU node sends said vehicle node a list with the key identifiers of the private keys shared by said vehicle node and the other vehicle nodes that have most recently contacted said RSU node for a predetermined period of time;
- said RSU node informs the VANET nodes, within a neighborhood of a predetermined number of hops from said RSU node, of the presence of said vehicle node and of the identifiers of keys obtained by said vehicle node;

such that two vehicle nodes are able to immediately establish a secure connection if there are shared keys between those two vehicles, without further

interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said two nodes.

2. Method according to the previous claim, wherein a sender node which is interested in communicating with a receiver node, if said sender node does not know the private keys held by the receiver node, comprises the step of both nodes broadcasting the key identifiers of the private keys held by each node, such that if there are shared keys then two nodes are then able to establish a secure connection, without further interaction, by deriving a new shared secret which is a cryptographic hash function of the keys shared by said vehicle node and one of the other vehicle nodes.

3. Method according to the previous claim, wherein if there are not shared keys between the two nodes, then the two nodes will establish a shared secret via standard PKC methods.

4. Method according to any previous claim, wherein if an RSU node or nodes are compromised, said method comprises the steps of:
   - the CA provides a new pool of keys to all RSU nodes that are not compromised, from which said pool of keys the vehicle nodes will then be able to obtain new keys;
   - the vehicle nodes are informed of the existence of the compromised RSU node or nodes.

5. Method according to any of the previous claims, wherein the private key identifiers are sequential IDs attributed as the private keys are generated.

6. Method according to any of the previous claims, for key distribution spanning multiple independent CA's, each CA with a predetermined geographical area, wherein the pool of private keys available to each RSU node is unique to a partitioned key space corresponding to the geographical area of each independent CA.

7. Method according to the previous claim, wherein the pool of private keys available to each RSU node comprises an additional key space that is parallel to said CA's and is thus shared by all CA's.

8. Method according to the previous claim, wherein said additional key space is made available by the RSU nodes only to vehicles that require communication between independent CAs.

9. Method according to any of the claims 6 - 8, wherein a vehicle node on moving from a first CA geographic region to a second CA geographic region, comprises the following steps:
   - before leaving said first CA geographic region, said vehicle node requests a set of keys from an RSU node that is within range and within that first CA region, indicating that those requested keys are for said second CA geographic region;
   - said RSU node then sends the vehicle node request to the first CA for a set of keys that can be used within the region controlled by the second CA;
   - the first CA forwards the vehicle node request to the second CA;
   - the second CA responds with a set of keys that can be used within the region controlled by the second CA with the respective list of identifiers which are sent to to the vehicle node encrypted with the vehicle node public key;

   such that such the vehicle node will be able to immediately establish a secure connection with any node in said second CA geographic region by deriving a new shared secret which is a cryptographic hash function of the keys shared by the two nodes.

10. Method according to the previous claim, wherein the RSU node is a RSU border node of first CA geographic region.

11. Device for key distribution by trusted nodes for a vehicular ad hoc network, VANET, wherein said vehicular ad hoc network is composed of nodes, a node being either a mobile vehicle node equipped with an on-board unit or a static road-side unit node, herewith referred respectively as vehicle nodes (A, B, C, D, E, F, G) and RSU nodes (R1, R2, R3), wherein said RSU nodes have a permanent

connection to a certificate authority, CA, said CA being responsible for a specific geographic region in which the VANET is comprised and said CA acting as the root of trust for the VANET, and wherein the VANET nodes have at least one pair of public-private keys and the corresponding certificates, issued by said CA, wherein each node comprises a data processing unit configured to carry out the method of any one of the previous claims.

12. Computer readable data carrier comprising the computer program instructions adapted to perform the method of any of the claims 1-10 when said program is run on a data processing unit.