What is claimed is:

~~1. An AAA server operated by, or on behalf of a Dedicated Short-Range Communications infrastructure authority, transmitting messages among and between On-board Units (OBU) and Roadside Units (RSU), said AAA server comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, with a plurality of RSUs, in order to carry out the functions of Authentication, Authorization and Accounting (AAA), enabling the authority to account for Wireless Access Vehicular Environment service channel bandwidth consumption by each of said user devices having been duly provisioned by said AAA server.~~

~~2~~1. An AAA server operated by, or on behalf of a Dedicated Short-Range Communications infrastructure authority, transmitting messages among and between On-board Units (OBU) and Roadside Units (RSU), said AAA server comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, with a plurality of RSUs, in order to carry out the functions of Authentication, Authorization and Accounting (AAA), enabling the authority to authenticate said user devices and/or said OBU, and to authorize said user devices and/or said OBU for access to any service subscribed thereby;

wherein the AAA server is operable to request assistance from Security Credentials and Management System (SCMS) components in validating the security credentials of said user devices and/or said OBU.

~~3. An AAA server as defined in claim 1 or claim 2, configured as a Certificate Management Entity and operable to issue Internet Subscription digital certificates for IPv6-addressable user devices and to~~

~~transmit said certificates to said user devices over a secure communications channel, said certificates including the domain name of said AAA server.~~

~~4. An AAA server as defined in any of claims 1 to 3, linked to a PKI chain of trust between components of a Security Credentials and Management System (SCMS), operable to process requests from DSRC OBUs for said digital certificates, said requests encapsulating Personal Identifying Information (PII) for said OBUs and secured by the asymmetrical encryption algorithm specified in IEEE 1609.2, using an enrollment certificate issued to said OBUs by the SCMS and operable to establish said secure communications channel for sending said certificate to said OBU using the encryption key of said enrollment certificate.~~

~~5. An AAA server as defined in any of claims 1 to 4, operable to process requests from non-DSRC mobile devices for said digital certificates, said requests encapsulating PII for said mobile device, each mobile device initiating a handshaking protocol to establish a secure, symmetrically encrypted communications channel with said AAA server.~~

~~6~~2. An AAA server as defined in ~~any of~~ claim~~s~~ 1 ~~to 5~~, operable to receive combined authorization and authentication requests from OBUs, said requests incorporating credentials in the form of digital signatures generated using keys ~~from said digital certificates or said Internet Subscription certificates issued to said OBUs by said AAA server~~ or from Enrollment certificates or similar issued to said OBUs by said SCMS; operable to receive said combined authorization and authentication requests forwarded from one or more remote AAA servers on behalf of OBUs that have received said digital certificates or said Internet Subscription certificates from said remote AAA servers or said Enrollment certificates from said SCMS; operable to process requests from both said OBUs and said remote AAA servers by cryptographic validation of the credentials presented correspondingly by said OBUs and said remote

AAA servers, for each request querying a non-remote AAA database for a match with PII contained in the request, and returning a message to the requesting OBU or remote AAA, either granting or denying authorization with a code representing a reason for denial.

~~7~~3. An AAA server as defined in ~~any of~~ claim~~s~~ 1 or 2 ~~to~~ 5~~6~~, operable to receive authorization requests from said OBUs on behalf of non-DSRC mobile devices, to send UDP/IP authentication challenge messages directly or indirectly to IPv6 address of said non-DSRC mobile devices; to process responses to said authentication challenges which incorporate credentials in the form of digital signatures generated using keys from said digital certificates or said Internet Subscription certificates issued to said non-DSRC mobile devices by said AAA server; and operable to receive said authorization requests forwarded from a remote AAA server on behalf of non-DSRC mobile devices that have received Internet Subscription credentials from said AAA server; operable to process said requests from both non-DSRC mobile devices and remote AAA servers by cryptographic validation of the credentials presented, querying the local AAA database for a match with PII contained in the request, and returning a message to the requester either granting or denying authorization with a code explaining the reason for denial.

~~8~~4. An AAA server as defined in any of claims 1 to 3~~7~~, operable, in the case where the domain name of the Certificate Management Entity having issued credentials used by a user device to request authentication and authorization, identifies a remote AAA server, to forward said request to said remote AAA server, using credentials obtained from said SCMS chain of trust to secure communications with said remote AAA server.

~~9~~5. An AAA server as defined in any of claims 1 to ~~8~~4, operable, in the case where the domain name of the Certificate Management Entity having issued the credentials used by a user device to respond to an authentication challenge from said AAA server, identifies a remote AAA server, to forward said request

to said remote AAA server, using credentials obtained from said SCMS chain of trust to secure communications with said remote AAA server.

~~10~~6. An AAA server as defined in any of claims 1 to ~~5~~9, operable to use Remotely Triggered Black Hole (RTBH) filtering with internal Border Gateway Protocol to send UPDATE messages to RSUs within a same Autonomous System, said UPDATE messages being triggered by, and encapsulating the results of an authentication and authorization request for Internet Subscription services received from a user device, said results being either the failure to authenticate said mobile device, or the granting or denial of authorization to said user device.

~~11~~7. An AAA server as defined in any of claims 1 to ~~6~~10, wherein, on receipt of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES is used to encrypt, and to transmit to the requesting device, the necessary parameters and keying material for symmetric encryption of the payload of the multicast "push notifications" provided by said multicast service.

~~12. A system facilitating communication between and among On-board Units (OBU) and Roadside Units (RSU) utilizing Dedicated Short-Range Communications (DSRC) to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, said system comprising:~~

~~a server transmitting messages among and between the OBU and the RSU, said server comprising at least one processor running at least one computer program adapted to authenticate the user device, authorize the user device to have access to Wireless Access Vehicular Environment (WAVE) service channels, and account for bandwidth consumption by each of said user devices having been duly authenticated and authorized by said AAA server.~~

~~13~~8. A system ~~as defined in claim 12,~~ comprising a plurality of AAA S~~s~~ervers, as defined in claim 5, operated by, or on behalf of a Dedicated Short-Range Communications (DSRC) infrastructure authority.

~~14. A system as defined in any of claims 1 to 13.~~