Claims

What is claimed:

1. A method of operation (400) of a wireless device (100) attached to a third partnership project, 3GPP, network, for establishing a Packet Data Unit, PDU, session over a non 3GPP access, comprising:
   - sending a Non-Access Stratum, NAS PDU session request message to establish a PDU session for transporting data of a particular type over an established Internet Protocol Security, IPsec, Security Association, SA;
   - establishing an IPSec Child SA, for the PDU session and using at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier for associating the IPSec Child SA to the established PDU session; and
   - encapsulating data to be transmitted for the PDU session using a Generic Encapsulation Header and adding to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.
2. The method of claim 1 wherein the PDU session request includes an application type or an application identifier of an application generating the data for the PDU session.
3. The method of claim 1 wherein the step of establishing the IPSec Child SA further comprises receiving an Internet Key Exchange, IKE Create_Child SA request message of an IKE Child SA exchange.
4. The method of claim 1 wherein the step of establishing the IPSec Child SA further comprises sending an IKE Create_Child SA request message of the IKE Child SA exchange.
5. The method of claim 3 or 4 wherein the method further comprises obtaining the IP address assigned to the PDU session during the IKE Child SA exchange.
6. The method of claims 1 and 5 wherein associating the IPSec Child SA to the PDU session further comprises correlating the IP address obtained in the IKE Child SA exchange to an IP address assigned to the PDU session and received in a PDU session response in response to the PDU session request.
7. The method of claim 1, where in the method further comprises receiving a PDU session response in response to the PDU session request and the PDU session response comprises the security parameter Index, SPI, of the IPSec Child SA.
8. The method of claim 7, wherein associating the IPSec Child SA to the PDU session further comprises correlating the SPI received in the IKE Child SA exchange to the SPI received in the PDU session response.
9. The method of claim 1, wherein sending the PDU session is initiated as a result of receiving the data from an Internet of Thing, IoT, device connected to the wireless device 100.
10. The method of claim 1, wherein the data of the particular type comprises one of non-Internet Protocol, non-IP framed data, non-IP raw data and IP data.

11. The method of claim 1, wherein the NAS PDU session request and any other NAS message is encapsulated in a Generic Encapsulation Header when transmitted as in an ESP frame over the established IPSec SA.
12. A wireless device (100), comprising:
    - at least one transceiver;
    - at least one processor; and
    - memory comprising instructions executable by the at least one processor whereby the wireless device (100) is operable to:
        - send a Non-Access Stratum Packet Data Unit, NAS PDU session request to establish a PDU session to transport data of a particular type over an established Internet Protocol Security, IPsec, Security Association, SA;
        - establish an IPSec Child SA, for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier to associate the IPSec Child SA to the established PDU session; and
        - encapsulate data to be transmitted for the PDU session using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.
13. A wireless device (100) adapted to:
    - send a Non-Access Stratum Packet Data Unit, NAS PDU session request to establish a PDU session to transport data of a particular type over an established Internet Protocol Security, IPsec, Security Association, SA;
    - establish an IPSec Child SA, for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier to associate the IPSec Child SA to the established PDU session; and
    - encapsulate data to be transmitted for the PDU session using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.
14. The wireless device (100) of claim 13 adapted to operate according to the method of any one of claims 2 to 11.
15. A wireless device (100) comprising:
    - a session management module (810) configured to:
        - send a PDU session request to establish a PDU session to transport data of a particular type over an established Internet Protocol Security, IPsec, Security Association, SA;
    - the security module (810) configured to:
        - establish an IPSec Child SA, for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a

PDU session identifier to associate the IPSec Child SA to the established PDU session; and

- an encapsulation module (810) configured to:
  - encapsulate data to be transmitted for the PDU session using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.

16. A computer program comprising instructions which, when executed on at least one processor, cause the at least one processor to carry out the method according to any one of embodiments 2 to 11.
17. A carrier containing the computer program of claim 16, wherein the carrier is one of an electronic signal, an optical signal, a radio signal, or a computer readable storage medium.
18. A wireless device (100) adapted to:

- send a Non Access Stratum, NAS, Packet Data Unit, PDU session request over an established Internet Protocol Security, IPsec, Security Association, SA to establish a PDU session for one of non-Internet Protocol, non-IP, data or IP data;
- receive a PDU session response in response to the NAS PDU session request; and
- encapsulate the one of non-IP data or IP data using a Generic Encapsulation Header and transmitting the one of encapsulated non-IP data or IP data in encapsulated security payload, ESP, frame associated with the established IPSec SA.

19. The wireless device (100) of claims 23 and 24 wherein the NAS PDU session request and other NAS messages are transmitted encapsulated in GRE and further encapsulated in an ESP frame corresponding to the established IPSec SA.
20. A network entity (103), comprising:

- at least one processor; and
- memory comprising instructions executable by the at least one processor whereby the network entity (103) is operable to:
  - receive a Non Access Stratum, Packet Data Unit, NAS PDU, session request from a UE (100) to establish a PDU session to transport data of a particular type over over an Internet Protocol Security, IPsec, Security Association, SA established with the UE (100);
  - establish an IPSec Child SA for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier to associate the IPSec Child SA to the established PDU session; and
  - encapsulate data to be transmitted for the PDU session to the UE using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA and indicate the type of data to be transmitted as the data of the particular type.

21. A network entity (103) adapted to:

- receive a Non Access Stratum, Packet Data Unit, NAS PDU, session request from a UE (100) to establish a PDU session to transport data of a particular type over an Internet Protocol Security, IPsec, Security Association, SA established with the UE (100);
- establish an IPSec Child SA for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier to associate the IPSec Child SA to the established PDU session; and
- encapsulate data to be transmitted to the UE for the PDU session using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.

22. The network entity (103) of claim 21, wherein the network entity (103) indicates the type of data by setting a next header field in ESP to a value corresponding to the data of the particular type.
23. The network entity (103) of claim 21, wherein the PDU session request includes an application type or an application identifier of an application generating the non-IP data for the PDU session.
24. The network entity (103) of claim 21, wherein the network entity (103) is further adapted to receive an Internet Key Exchange, IKE Create_Child SA request message of an IKE Child SA exchange in order to establish the IPSec Child SA for the PDU session.
25. The network entity (103) of claim 21, wherein the network entity (103) is further adapted to receive an Internet Key Exchange, IKE Create_Child SA request message of an IKE Child SA exchange in order to establish the IPSec Child SA for the PDU session.
26. A network entity (103) comprising:

- a receiving module (820) configured to:
  - receive a Non Access Stratum, Packet Data Unit, NAS PDU, session request from a UE (100) to establish a PDU session to transport data of a particular type over over an Internet Protocol Security, IPsec, Security Association, SA established with the UE (100);
- a security module (820) configured to:
  - establish an IPSec Child SA for the PDU session and use at least one of a security parameter Index of the IPSec Child SA, an IP address assigned to the PDU session or a PDU session identifier to associate the IPSec Child SA to the established PDU session; and
- an encapsulation module (820) configured to:
  - encapsulate data to be transmitted to the UE for the PDU session using a Generic Encapsulation Header and add to the encapsulated data an Encapsulation Security Payload, ESP, frame corresponding to the IPSec Child SA wherein a type of encapsulated data is provided and the type corresponds to the particular type of data identified for the PDU session.

27. A network entity (103) adapted to:

- receive a Non Access Stratum, NAS, Packet Data Unit, PDU session request over an established Internet Protocol Security, IPsec, Security Association, SA to establish a PDU

session for a User Equipment (100) to transport one of non-Internet Protocol, non-IP, data or IP data, the NAS PDU session request is encapsulated in an Encapsulated Security Payload, ESP frame;

- send a NAS PDU session response that indicates that the one of non-IP data or IP data of the PDU session is to be encapsulated by Generic Routing Encapsulation, GRE, in the ESP frame; and
- encapsulate the one of non-IP data or IP data in a header of the inner encapsulation and transmit to the UE (100) the one of encapsulated non-IP data or IP data in the ESP frame.

28. The network entity (103) of claim 31 wherein the NAS PDU session response and other NAS messages are transmitted encapsulated in GRE and further encapsulated in an ESP frame corresponding to the established IPSec SA.