protection for control plane messages.

Summary

Embodiments described herein provide enhanced protection for NAS messages. A NAS procedure (e.g., registration of a UE) includes a set of Information Elements (IEs) that carry information. The embodiments described below set forth ways of protecting the IEs or a subset of the IEs that are sent in NAS messages. Thus, the information carried in the IEs is less vulnerable to malicious attacks.

In an aspect there is provided a User Equipment (UE) comprising:

at least one processor; and

at least one memory storing instructions that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an IDLE mode to a CONNECTED mode and the UE does not have a security context for communication with a network element of a mobile network, initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element of the mobile network,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during a first phase of the NAS procedure:

constructing a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;

sending the first initial NAS message to the network element; and

receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during a second phase of the NAS procedure:

constructing a subsequent NAS message, the subsequent NAS message including a NAS message container, the NAS message container comprising a second initial NAS message contained therein, the second initial NAS message comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during initiation of the NAS procedure to establish the NAS communication session between the UE and the network element and one or more additional NAS protocol IEs; and

sending the subsequent NAS message to the network element.

In an aspect there is provided a network element configured for communication in a mobile network, the network element comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the network element to perform at least:

in an instance in which a security context does not exist for communication between the network element and a user equipment (UE) in the mobile network, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a first phase of the NAS procedure:

receiving, from the UE, a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) selected from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a second phase of the NAS procedure:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a NAS message container, wherein the NAS message container comprises a second initial NAS message encapsulated within the NAS message container, wherein the second initial NAS message defines a same message type as the first initial NAS message and comprises the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, wherein the NAS message container of the subsequent NAS message is encrypted using the NAS security algorithm provided to the UE during the first phase of the NAS procedure.

In an aspect there is provided a method comprising:
in an instance in which a user equipment (UE) is transitioning from an IDLE mode to a CONNECTED mode, and the UE does not have a security context for communication with a network element of a mobile network, initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and a network element of a mobile network,
wherein, during a first phase of the NAS procedure, said initiating comprises:
constructing a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;
sending the first initial NAS message to the network element; and
receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and
wherein, during a second phase of the NAS procedure, said initiating comprises:
generating a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein a second initial NAS message is encapsulated within the NAS message container, wherein the second initial NAS message defines a same message type as the first initial NAS message, and wherein the second initial NAS message includes the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs; and
sending the subsequent NAS message to the network element.

In an aspect there is provided a method comprising:
in an instance in which an Access and Mobility Management Function (AMF) of a mobile network determines that a security context does not exist for communication between the AMF and a user equipment (UE) in the mobile network and the UE is transitioning from an IDLE mode to a CONNECTED mode, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the AMF, wherein the carrying out the NAS procedure comprises, during a first phase of the NAS procedure:

receiving, via a network interface component of the AMF, from the UE, a first initial NAS message, the first initial NAS message containing a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs for use during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

sending, using the AMF, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE when communicating with the mobile network, and

wherein the carrying out the NAS procedure further comprises, during a second phase of the NAS procedure:

receiving, via the network interface component of the AMF, a subsequent NAS message generated by the UE, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container of the subsequent NAS message, the second initial NAS message defining a same message type as the first initial NAS message, the second initial NAS message including the full set of NAS protocol IEs for the NAS procedure including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional IEs, wherein the NAS message container of the subsequent NAS message is encrypted using the NAS security algorithm provided to the UE during the first phase of the NAS procedure.

In an aspect there is provided a User Equipment (UE) comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an IDLE mode to a CONNECTED mode and the UE does not have a security context for communication with a network element of a mobile network, constructing a first initial Non-Access Stratum (NAS) message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) selected from among a full set of NAS protocol IEs for use during a NAS registration procedure, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS registration procedure;

sending the first initial NAS message to the network element of the mobile network;
receiving, in response to the first initial NAS message, from the network element, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE;
in response to receiving the NAS security algorithm and the security key set identifier associated with the NAS security context, constructing a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein the NAS message container encapsulates therein the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, and wherein the second initial NAS message defines a same message type as the first initial NAS message; and
sending the subsequent NAS message to the network element.

In an aspect there is provided an Access and Mobility Management Function (AMF) configured for communication within a mobile network, the AMF comprising:
at least one processor; and
at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the AMF to perform at least:
in an instance in which the AMF determines that a security context does not exist for communication between the AMF and a user equipment (UE) in the mobile network and the UE is transitioning from an IDLE mode to a CONNECTED mode, carrying out a Non-Access Stratum (NAS) procedure to establish a NAS communication session between the UE and the AMF by performing:
receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure;
sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE; and
receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container of the

subsequent NAS message, the second initial NAS message defining a same message type as the first initial NAS message, the second initial NAS message including the full set of NAS protocol IEs for the NAS procedure including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs.

In an aspect there is provided a user equipment (UE) comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an idle mode to a connected mode, and the UE does not have a security context for communication with a network element of a mobile network, initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element of the mobile network,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the UE to perform, during a first phase of the NAS procedure:

identifying, from among a full set of NAS protocol Information Elements (IEs) used during the NAS procedure, a subset of NAS protocol IEs, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;

inserting, into the first initial NAS message, the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure;

sending the first initial NAS message to the network element; and

receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the UE to perform, during a second phase of the NAS procedure:

generating a second initial NAS message;

inserting, into the second initial NAS message, the full set of NAS protocol IEs for use during the NAS procedure, including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, wherein the second initial NAS message defines a same message type as the first initial NAS message;

generating a subsequent NAS message comprising a NAS message container;

inserting the second initial NAS message into the NAS message container of the subsequent NAS message;

encrypting the NAS message container in the subsequent NAS message using the NAS security algorithm received at the UE from the network element in response to the first initial NAS message; and

sending the subsequent NAS message to the network element.

In an aspect there is provided a network element configured for communication within a mobile network, the network element comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the network element to perform at least:

in an instance in which a user equipment (UE) is transitioning from an idle mode to a connected mode, and the network element determines that the UE does not have a security context for communication with the network element, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the network element to perform, during a first phase of the NAS procedure:

receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) selected from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure to

establish the NAS communication session between the UE and the network element; and

sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a second phase of the NAS procedure:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein a second initial NAS message is encapsulated within the NAS message container of the subsequent NAS message, wherein the second initial NAS message defines a same message type as the first initial NAS message, and wherein the second initial NAS message comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs.

In an example there is provided a User Equipment (UE) comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processor, cause the UE to initiate a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and a network element of a mobile network,

wherein, in a first phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

constructs a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

sends the first initial NAS message to the network element; and

receives a response from the network element that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE, and

wherein, in a second phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

constructs a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sends the subsequent NAS message to the network element.

In an example, there is provided network element of a mobility network comprising:

at least one processor; and

at least one memory including computer program code, the at least one memory and the computer program code being configured to, with the at least one processor, cause the network element to carry out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and the network element,

wherein, in a first phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

receive, from the UE, a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

construct a response to the first initial NAS message that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE; and

send, to the UE, the response to the first initial NAS message, and

wherein, in a second phase of the NAS procedure, the at least one memory and the computer program code are configured, with the at least one processor, to:

receive, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs.

In an aspect there is provided a method comprising:

initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and a network element of a mobile network,

wherein, in a first phase of the NAS procedure, said initiating comprises:

constructing a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

sending the first initial NAS message to the network element; and

receiving a response from the network element that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE, and

wherein, in a second phase of the NAS procedure, said initiating comprises:

constructing a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sending the subsequent NAS message to the network element.

In an example, there is provided a method comprising:

causing a network element of a mobile network to carry out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between user equipment (UE) and the network element,

wherein, in a first phase of the NAS procedure, said causing comprises:

receiving, from the UE, a first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling;

constructing a response to the first initial NAS message that includes a NAS security algorithm and security key set identifier associated with a NAS security context for use by the UE; and

sending, to the UE, the response to the first initial NAS message, and

wherein, in a second phase of the NAS procedure, said causing comprises:

constructing a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure which is different from the first set of NAS protocol IEs; and

sending the subsequent NAS message to the network element.

In an example, there is User Equipment (UE) comprising:

at least one processor; and

at least one memory including computer program code; the at least one memory and the computer program code being configured to, with the at least one processor, cause the UE to initiate and perform a Non-Access Stratum (NAS) procedure to establish a NAS communication session between the UE and a network element of a mobile network;

wherein the at least one memory and the computer program code are configured, with the at least one processor, to:

determine that a NAS security context exists for use by the UE;

construct a first initial NAS message, the first initial NAS message including a first set of NAS protocol Information Elements (IEs) that are designated for security-related handling, the first initial NAS message further including a second initial NAS message encapsulated within a NAS message container IE, the second initial NAS message defining a same message type as the first initial NAS message and including a second set of NAS protocol IEs for the NAS procedure, which is different from the first set of NAS protocol IEs; and

send the first initial NAS message to the network element.

One example comprises a network element of a mobile network. The network element includes a processor(s), and memory including computer program code executable by the processor. The processor is configured to cause the network element to perform a NAS procedure in multiple phases to establish a NAS communication session between the network element and a UE. For a first phase of the NAS procedure, the processor is further configured to cause the network element to receive an initial NAS message from the UE, where the initial NAS message is populated with a subset of NAS protocol IEs, from the NAS protocol IEs for the NAS procedure, that are designated for security-related handling. The processor is further configured to cause the network element to process the subset of the NAS protocol IEs to determine that a NAS security context does not exist for the UE, select a NAS security algorithm for the NAS security context, and send a response to the UE that indicates the NAS security algorithm and a security key set identifier of the NAS security context. For a second phase of the NAS procedure, the processor is further configured to cause the network element to receive a subsequent NAS message from the UE having a NAS message container that contains the initial NAS message encrypted based on the NAS security algorithm, and decrypt the NAS message container of the subsequent NAS message,

where the initial NAS message contained in the NAS message container of the subsequent NAS message is populated with each of the NAS protocol IEs for the NAS procedure.

In another example, for the first phase, the subset of the NAS protocol IEs are encrypted in the initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE. The processor is further configured to cause the network element to initiate decryption of the subset of the NAS protocol IEs.

What is claimed is:

1. User Equipment (UE) comprising:

at least one processor; and

at least one memory storing instructions that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an IDLE mode to a CONNECTED mode and the UE does not have a security context for communication with a network element of a mobile network, initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element of the mobile network,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during a first phase of the NAS procedure:

constructing a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;

sending the first initial NAS message to the network element; and

receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during a second phase of the NAS procedure:

constructing a subsequent NAS message, the subsequent NAS message including a NAS message container, the NAS message container comprising a second initial NAS message contained therein, the second initial NAS message comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists

only of those NAS protocol IEs that are designated for security-related handling during initiation of the NAS procedure to establish the NAS communication session between the UE and the network element and one or more additional NAS protocol IEs; and

sending the subsequent NAS message to the network element.

2. The UE of claim 1, wherein the instructions stored at the at least one memory, when executed by the at least one processor, further cause the UE to perform:

determining whether the UE has a security context for communication with the network element of the mobile network.

3. The UE of claim 1, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during the first phase of the NAS procedure:

identifying, from among the full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs that consist only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

inserting, into the first initial NAS message, the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element.

4. The UE of claim 1, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform, during the first phase of the NAS procedure:

encrypting the subset of NAS protocol IEs in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

5. The UE of claim 1, wherein the instructions stored at the at least one memory, when executed by the at least one processor, further cause the UE to perform said generating the subsequent NAS message by:

inserting, in the second initial NAS message, the full set of NAS protocol IEs used during the NAS procedure, including the subset of NAS protocol IEs that consists only of

those NAS protocol IEs designated for security-related handling during initiation of the NAS procedure to establish the NAS communication session between the UE and the network element, the second initial NAS message defining a same message type as the first initial NAS message;

inserting the second initial NAS message in a NAS message container of the subsequent NAS message; and

encrypting the NAS message container of the subsequent NAS message using the NAS security algorithm received from the network element during the first phase of initiation of the NAS procedure.

6. The UE of claim 1, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform at least:

in an instance in which the UE has a public key programmed on a Universal Mobile Telecommunications System (UMTS) Subscriber Identify Module (USIM) of the UE, encrypting the subset of the NAS protocol IEs in the first initial NAS message using the public key programmed on the USIM of the UE; and

in an instance in which the UE does not have the public key programmed on the USIM of the UE, sending the first initial NAS message to the network element without encrypting the subset of NAS protocol IEs in the first initial NAS message.

7. The UE of claim 1, wherein the first initial NAS message comprises a registration request message.

8. The UE of claim 1, wherein the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

9. The UE of claim 8, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform at least:

in an instance in which the registration type in the subset of NAS protocol IEs does not indicate an emergency, encrypting the subset of NAS protocol IEs in the first initial NAS

message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE; and

in an instance in which the registration type in the subset of NAS protocol IEs indicates an emergency, refraining from encrypting the subset of NAS protocol IEs in the first initial NAS message before sending the first initial NAS message to the network element.

10. The UE of claim 1, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are received in a security mode command message, wherein the subsequent NAS message comprises a security mode complete message comprising the NAS message container that contains the second initial NAS message, and wherein the second initial NAS message in the subsequent NAS message is encrypted based on the NAS security algorithm received at the UE during the first phase of the NAS procedure.

11. A network element configured for communication in a mobile network, the network element comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the network element to perform at least:

in an instance in which a security context does not exist for communication between the network element and a user equipment (UE) in the mobile network, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a first phase of the NAS procedure:

receiving, from the UE, a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) selected from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a second phase of the NAS procedure:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a NAS message container, wherein the NAS message container comprises a second initial NAS message encapsulated within the NAS message container, wherein the second initial NAS message defines a same message type as the first initial NAS message and comprises the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, wherein the NAS message container of the subsequent NAS message is encrypted using the NAS security algorithm provided to the UE during the first phase of the NAS procedure.

12. The network element of claim 11, wherein the subset of NAS protocol IEs, which consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure, are encrypted by the UE using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

13. The network element of claim 11, wherein the first initial NAS message comprises a registration request message.

14. The network element of claim 11, wherein the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure, comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

15. The network element of claim 11, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are received in a

security mode command message, and wherein the subsequent NAS message comprises a security mode complete message, the security mode complete message comprising the NAS message container that encapsulates therein the second initial NAS message, the second initial NAS message being encrypted based on the NAS security algorithm provided to the UE during the second phase of the NAS procedure.

16. A method comprising:

in an instance in which a user equipment (UE) is transitioning from an IDLE mode to a CONNECTED mode, and the UE does not have a security context for communication with a network element of a mobile network, initiating, by the UE, a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and a network element of a mobile network,

wherein, during a first phase of the NAS procedure, said initiating comprises:

constructing a first initial NAS message, the first initial NAS message comprising a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;

sending the first initial NAS message to the network element; and

receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein, during a second phase of the NAS procedure, said initiating comprises:

generating a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein a second initial NAS message is encapsulated within the NAS message container, wherein the second initial NAS message defines a same message type as the first initial NAS message, and wherein the second initial NAS message includes the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs; and

sending the subsequent NAS message to the network element.

17. The method of claim 16, further comprising:

determining whether the UE has a security context for communication with the network element of the mobile network.

18. The method of claim 16, further comprising, during the first phase of the NAS procedure:

identifying, from among the full set of NAS protocol IEs used during the NAS procedure, the subset of NAS protocol IEs that consist only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

inserting, into the first initial NAS message, the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element.

19. The method of claim 16, further comprising, during the first phase of the NAS procedure:

encrypting the subset of NAS protocol IEs in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

20. The method of claim 16, further comprising:

inserting, in the second initial NAS message, the full set of NAS protocol IEs used during the NAS procedure, including the subset of NAS protocol IEs that consists only of those NAS protocol IEs designated for security-related handling during initiation of the NAS procedure to establish the NAS communication session between the UE and the network element, the second initial NAS message defining a same message type as the first initial NAS message;

inserting the second initial NAS message in a NAS message container of the subsequent NAS message; and

encrypting the NAS message container of the subsequent NAS message using the NAS security algorithm received from the network element during the first phase of initiation of the NAS procedure.

21. The method of claim 16, further comprising:

in an instance in which the UE has a public key programmed on a Universal Mobile Telecommunications System (UMTS) Subscriber Identify Module (USIM) of the UE, encrypting the subset of the NAS protocol IEs in the first initial NAS message using the public key programmed on the USIM of the UE; and

in an instance in which the UE does not have the public key programmed on the USIM of the UE, sending the first initial NAS message to the network element without encrypting the subset of NAS protocol IEs in the first initial NAS message.

22. The method of claim 16, wherein the first initial NAS message comprises a registration request message.

23. The method of claim 16, wherein the subset of NAS protocol IEs consisting only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

24. The method of claim 23, further comprising:

in an instance in which the registration type in the subset of NAS protocol IEs does not indicate an emergency, encrypting the subset of NAS protocol IEs in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE; and

in an instance in which the registration type in the subset of NAS protocol IEs indicates an emergency, refraining from encrypting the subset of NAS protocol IEs in the first initial NAS message before sending the first initial NAS message to the network element.

25. The method of claim 16, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are received in a security mode command message, wherein the subsequent NAS message comprises a security mode complete message comprising the NAS message container that contains the second initial NAS message, and wherein the second initial NAS message in the subsequent NAS message

is encrypted based on the NAS security algorithm received at the UE during the first phase of the NAS procedure.

26. A method comprising:

in an instance in which an Access and Mobility Management Function (AMF) of a mobile network determines that a security context does not exist for communication between the AMF and a user equipment (UE) in the mobile network and the UE is transitioning from an IDLE mode to a CONNECTED mode, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the AMF,

wherein the carrying out the NAS procedure comprises, during a first phase of the NAS procedure:

receiving, via a network interface component of the AMF, from the UE, a first initial NAS message, the first initial NAS message containing a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs for use during the NAS procedure, the subset of NAS protocol IEs consisting only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

sending, using the AMF, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE when communicating with the mobile network, and

wherein the carrying out the NAS procedure further comprises, during a second phase of the NAS procedure:

receiving, via the network interface component of the AMF, a subsequent NAS message generated by the UE, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container of the subsequent NAS message, the second initial NAS message defining a same message type as the first initial NAS message, the second initial NAS message including the full set of NAS protocol IEs for the NAS procedure including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional IEs, wherein the NAS message container of the subsequent NAS message is

encrypted using the NAS security algorithm provided to the UE during the first phase of the NAS procedure.

27. The method of claim 26, wherein the subset of NAS protocol IEs, which consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure, are encrypted by the UE using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

28. The method of claim 26, wherein the first initial NAS message comprises a registration request message.

29. The method of claim 26, wherein the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure, comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

30. The method of claim 26, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are received in a security mode command message, and wherein the subsequent NAS message comprises a security mode complete message, the security mode complete message comprising the NAS message container that encapsulates therein the second initial NAS message, the second initial NAS message being encrypted based on the NAS security algorithm provided to the UE during the second phase of the NAS procedure.

31. A User Equipment (UE) comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an IDLE mode to a CONNECTED mode and the UE does not have a security context for communication with a network element of a mobile network, constructing a first initial Non-Access Stratum (NAS) message, the first initial NAS message comprising a subset of NAS protocol Information

Elements (IEs) selected from among a full set of NAS protocol IEs for use during a NAS registration procedure, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS registration procedure;

sending the first initial NAS message to the network element of the mobile network;

receiving, in response to the first initial NAS message, from the network element, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE;

in response to receiving the NAS security algorithm and the security key set identifier associated with the NAS security context, constructing a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein the NAS message container encapsulates therein the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, and wherein the second initial NAS message defines a same message type as the first initial NAS message; and

sending the subsequent NAS message to the network element.

32. The UE of claim 31, wherein the second initial NAS message within the NAS message container of the subsequent NAS message is encrypted using the NAS security algorithm received by the UE in response to the first initial NAS message and associated with the NAS security context.

33. The UE of claim 31, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform:

identifying, from among the full set of NAS protocol IEs, the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure;

adding the subset of NAS protocol IEs to the first initial NAS message; and

encrypting the subset of NAS protocol IEs in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

34. The UE of claim 31, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform:

in an instance in which the UE has a public key programmed on a UMTS Subscriber Identity Module (USIM) of the UE, encrypting the subset of NAS protocol IEs in the first initial NAS message using the public key programmed on the USIM of the UE; and

in an instance in which the UE does not have the public key programmed on the USIM of the UE, refraining from encrypting the subset of NAS protocol IEs in the first initial NAS message before sending the first initial NAS message to the network element.

35. The UE of claim 31, wherein the first initial NAS message comprises a registration request message.

36. The UE of claim 31, wherein the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

37. The UE of claim 36, wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the UE to perform:

in an instance in which the registration type does not indicate an emergency, encrypting the subset of NAS protocol IEs in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE; and

in an instance in which the registration type indicates an emergency, sending the first initial NAS message to the network element without encrypting the subset of NAS protocol IEs in the first initial NAS message.

38. The UE of claim 31, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are received in a security mode command message.

39. The UE of claim 31, wherein the subsequent NAS message comprises a security mode complete message.

40. An Access and Mobility Management Function (AMF) configured for communication within a mobile network, the AMF comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the AMF to perform at least:

in an instance in which the AMF determines that a security context does not exist for communication between the AMF and a user equipment (UE) in the mobile network and the UE is transitioning from an IDLE mode to a CONNECTED mode, carrying out a Non-Access Stratum (NAS) procedure to establish a NAS communication session between the UE and the AMF by performing:

receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consists only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure;

sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE; and

receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container of the subsequent NAS message, the second initial NAS message defining a same message type as the first initial NAS message, the second initial NAS message including the full set of NAS protocol IEs for the NAS procedure including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs.

41. The network element of claim 40, wherein the second initial NAS message is encrypted within the NAS message container using the NAS security algorithm associated with the NAS security context.

42. The network element of claim 40, wherein the subset of NAS protocol IEs are encrypted in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

43. The network element of claim 42, wherein, in an instance in which the UE has a public key programmed on a UMTS Subscriber Identity Module (USIM) of the UE, the subset of NAS protocol IEs are encrypted in the first initial NAS message using the public key programmed on the USIM of the UE, and wherein, in an instance in which the UE does not have the public key programmed on the USIM of the UE, the subset of NAS protocol IEs are not encrypted in the first initial NAS message.

44. The network element of claim 40, wherein the first initial NAS message comprises a registration request message.

45. The network element of claim 40, wherein the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure comprises: a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, and a registration type.

46. The network element of claim 45, wherein, in an instance in which the registration type does not indicate an emergency, the subset of NAS protocol IEs, which consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure, are encrypted in the first initial NAS message using a public key of a Home Public Land Mobile Network (HPLMN) for the UE, and wherein, in an instance in which the registration type indicates an emergency, the subset of NAS protocol IEs, which consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure, are not encrypted in the first initial NAS message.

47. The network element of claim 40, wherein the NAS security algorithm and the security key set identifier associated with the NAS security context for use by the UE are provided to the UE in a security mode command message.

48. The network element of claim 40, wherein the subsequent NAS message comprises a security mode complete message.

49. A user equipment (UE) comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the UE to perform at least:

in an instance in which the UE is transitioning from an idle mode to a connected mode, and the UE does not have a security context for communication with a network element of a mobile network, initiating a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element of the mobile network,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the UE to perform, during a first phase of the NAS procedure:

identifying, from among a full set of NAS protocol Information Elements (IEs) used during the NAS procedure, a subset of NAS protocol IEs, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element;

inserting, into the first initial NAS message, the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure;

sending the first initial NAS message to the network element; and

receiving, from the network element, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE, and

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the UE to perform, during a second phase of the NAS procedure:

generating a second initial NAS message;

inserting, into the second initial NAS message, the full set of NAS protocol IEs for use during the NAS procedure, including the subset of NAS protocol IEs that consists only of those NAS protocol IEs that are designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs, wherein the second initial NAS message defines a same message type as the first initial NAS message;

generating a subsequent NAS message comprising a NAS message container;

inserting the second initial NAS message into the NAS message container of the subsequent NAS message;

encrypting the NAS message container in the subsequent NAS message using the NAS security algorithm received at the UE from the network element in response to the first initial NAS message; and

sending the subsequent NAS message to the network element.

50. A network element configured for communication within a mobile network, the network element comprising:

at least one processor; and

at least one memory comprising instructions stored thereon that, when executed by the at least one processor, cause the network element to perform at least:

in an instance in which a user equipment (UE) is transitioning from an idle mode to a connected mode, and the network element determines that the UE does not have a security context for communication with the network element, carrying out a Non-Access Stratum (NAS) procedure in multiple phases to establish a NAS communication session between the UE and the network element,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, cause the network element to perform, during a first phase of the NAS procedure:

receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) selected from among a full set of NAS protocol IEs for use during the NAS procedure, wherein the subset of NAS protocol IEs consist only of those NAS protocol IEs from among the full set of NAS protocol

IEs that are designated for security-related handling during the NAS procedure to establish the NAS communication session between the UE and the network element; and

sending, to the UE, in response to the first initial NAS message, a NAS security algorithm and a security key set identifier associated with a NAS security context for use by the UE,

wherein the instructions stored on the at least one memory, when executed by the at least one processor, further cause the network element to perform, during a second phase of the NAS procedure:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message comprising a NAS message container, wherein a second initial NAS message is encapsulated within the NAS message container of the subsequent NAS message, wherein the second initial NAS message defines a same message type as the first initial NAS message, and wherein the second initial NAS message comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs that consists only of those NAS protocol IEs designated for security-related handling during the NAS procedure and one or more additional NAS protocol IEs.