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 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, during a first phase of the NAS procedure, the instructions, when executed by the at least one processor, cause the UE to perform at least:
constructing a first initial NAS message, the first initial NAS message containing a first set of NAS protocol Information Elements (IEs) that includes only 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 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, during a second phase of the NAS procedure, the instructions, when executed by the at least one processor, further cause the UE to perform at least:
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, the second set of NAS protocol IEs including the first set of NAS protocol IEs 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 of a mobility network comprising:
at least one processor; and
at least one memory storing instructions that, when executed by 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, during a first phase of the NAS procedure, the instructions, when executed by the at least one processor, cause the network element to perform at least:
receiving, from the UE, a first initial NAS message, the first initial NAS message containing a first set of NAS protocol Information Elements (IEs) that includes only those NAS protocol IEs that are designated for security-related handling during the NAS procedure;
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, during a second phase of the NAS procedure, the instructions, when executed by the at least one processor, further cause the network element to perform:
receiving, 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, the second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional 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, during a first phase of the NAS procedure, said initiating comprises:
constructing a first initial NAS message, the first initial NAS message containing a first set of NAS protocol Information Elements (IEs) including only 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 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, during 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, the second set of NAS protocol IEs including the first set of NAS protocol IEs 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:

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

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

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, during 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, the second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional IEs; and

sending the subsequent NAS message to the network element.

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 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 by causing the UE to perform at least:
determining that a NAS security context exists for use by the UE;
constructing a first initial NAS message, the first initial NAS message containing an entire set of NAS protocol Information Elements (IEs) for the NAS procedure;
constructing a second initial NAS message defining a same message type as the first initial NAS message and including the entire set of NAS protocol IEs for the NAS procedure;
encapsulating the first initial NAS message in a NAS message container of the second initial NAS message; and
sending the second initial NAS message to the network element.

In an aspect there is provided a network element of a mobility network comprising:
at least one processor; and
at least one memory storing instructions that, when executed by the at least one processor, cause the network element to participate in performing a Non-Access Stratum (NAS) procedure to establish a NAS communication session between user equipment (UE) and the network element by causing the network element to perform at least:
receiving a second initial NAS message from the UE, the second initial NAS message containing an entire set of NAS protocol Information Elements (IEs) for the NAS procedure, the second initial NAS message further containing a first initial NAS message encapsulated within a NAS message container IE of the second initial NAS message, the first initial NAS message defining a same message type as the second initial NAS message and including the entire set of NAS protocol IEs for the NAS procedure.

In an aspect there is provided a method comprising:
causing user equipment (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 said causing comprises:
determining that a NAS security context exists for use by the UE;
constructing a first initial NAS message, the first initial NAS message containing an entire set of NAS protocol Information Elements (IEs) for the NAS procedure, including one or more NAS protocol IEs designated for security-related handling;

constructing a second initial NAS message containing a NAS message container and the entire set of NAS protocol IEs for the NAS procedure, including the one or more NAS protocol IEs designated for security-related handling;
encapsulating the first initial NAS message within the NAS message container of the second initial NAS message, the second initial NAS message defining a same message type as the first initial NAS message; and
sending the second initial NAS message to the network element.

In an aspect there is provided a method comprising:
causing a network element to participate in performing a Non-Access Stratum (NAS) procedure to establish a NAS communication session between user equipment (UE) and the network element;
wherein said causing comprises:
receiving a second initial NAS message from the UE, the second initial NAS message containing an entire set of NAS protocol Information Elements (IEs) for establishment of the NAS communication session, the second initial NAS message further containing a first initial NAS message encapsulated within a NAS message container IE of the second initial NAS message, the first initial NAS message defining a same message type as the second initial NAS message, the first initial NAS message containing the entire set of NAS protocol IEs for establishment of the NAS communication session.

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:
constructing a first initial Non-Access Stratum (NAS) message containing a first set of NAS protocol Information Elements (IEs) including only those NAS protocol IEs that are designated for security-related handling during a NAS procedure;
sending the first initial NAS message to a network element of a 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 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 and including a second set of NAS protocol IEs for a NAS procedure, the second set of NAS protocol IEs including the first set of NAS protocol IEs 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 of a mobility network comprising:
at least one processor; and
at least one memory storing instructions that, when executed by the at least one processor, cause the network element to perform at least:
receiving, from a user equipment (UE), a first initial Non-Access Stratum (NAS) message containing a first set of NAS protocol Information Elements (IEs) that include only those NAS protocol IEs that are designated for security-related handling during a NAS procedure;
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;
sending, to the UE, the response to the first initial NAS message; 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 and including a second set of NAS protocol IEs for the NAS procedure, the second set of NAS protocol IEs including the first set of NAS protocol IEs 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 storing instructions that, when executed by the at least one processor, cause the UE to perform at least:
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, the instructions, when executed by the at least one processor, cause the UE to perform:

identifying, from among an entire set of NAS protocol Information Elements (IEs) used during the NAS procedure, a subset of NAS protocol IEs that include only 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;
inserting the subset of NAS protocol IEs, including only those NAS protocol IEs that are designated for security-related handling during initiation of the NAS procedure, into a first initial NAS message;
sending the first initial NAS message to the network element; and
receiving, in response to the first initial NAS message, from the network element, a response message that includes a NAS security algorithm and 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, the instructions, when executed by the at least one processor, cause the UE to perform:
inserting the entire set of NAS protocol IEs for the NAS procedure, including the subset of NAS protocol IEs that includes only those NAS protocol IEs that are designated for security-related handling during initiation of the NAS procedure, and one or more additional NAS protocol IEs, into a second initial NAS message, 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 a subsequent NAS message;
encrypting the NAS message container of the subsequent NAS message using the NAS security algorithm received 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 of a mobility network comprising:
at least one processor; and
at least one memory storing instructions that, when executed by the at least one processor, cause the network element to perform at least:
carrying 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, during a first phase of the NAS procedure, the instructions, when executed by the at least one processor, cause the network element to perform:

receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) selected from among an entire set of NAS protocol IEs, the subset of NAS protocol IEs including only 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;

constructing a response to the first initial NAS message that includes a NAS security algorithm and a 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, during a second phase of the NAS procedure, the instructions, when executed by the at least one processor, cause the network element to perform:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE 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 comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs and one or more additional NAS protocol IEs.

In an ~~aspect~~ 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~~aspect~~, 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~~aspect~~, 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~~aspect~~, 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 ~~embodiment~~ 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~~embodiment~~, 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 ~~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~~ during a first phase of the NAS procedure, the instructions, when executed by ~~at least one memory and the computer program code are configured, with~~ the at least one processor, cause the UE to perform at least:

~~constructs~~ constructing a first initial NAS message, the first initial NAS message containing ~~including~~ a first set of NAS protocol Information Elements (IEs) that includes only those NAS protocol IEs that are designated for security-related handling during the NAS procedure;

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

~~receives~~ 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~~ during a second phase of the NAS procedure, the instructions, when executed by ~~at least one memory and the computer program code are configured, with~~ the at least one processor, further cause the UE to perform at least:

~~constructs~~ 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 second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional NAS protocol IEs; and

~~sends~~ sending the subsequent NAS message to the network element.

2. The UE of claim 1, wherein, ~~in~~ during the second phase of the NAS procedure, the second initial NAS message is encrypted within the NAS message container using the NAS security algorithm received ~~in~~ during the first phase of the NAS procedure.

~~3. The UE of claim 1, wherein, in the second phase of the NAS procedure, the second set of NAS protocol IEs includes the NAS protocol IEs in the first set of NAS protocol IEs and one or more additional NAS protocol IEs.~~

34. The UE of claim 1, wherein, ~~in~~ during the first phase of the NAS procedure, the instructions, when executed by ~~at least one memory and the computer program code are further configured, with~~ the at least one processor, further cause the UE to perform at least:

~~identify,~~ identifying, from among the first set of NAS protocol IEs, a subset of the NAS protocol IEs that include only those NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

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

~~insert the subset of the NAS protocol IEs into the first initial NAS message~~.

~~5~~4. The UE of claim ~~4~~3, wherein the instructions, when executed by ~~at least one memory and the computer program code are further configured, with~~ the at least one processor, further cause the UE to perform at least:

encrypting the subset of the NAS protocol IEs in the first initial NAS message using a public key when the UE has the public key programmed on a UMTS Subscriber Identify Module (USIM); and

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

~~6~~5. The UE of claim ~~4~~3, wherein:

the first initial NAS message comprises a registration request message; and

the subset of NAS protocol IEs comprising only those NAS protocol IEs that are designated for security-related handling during the NAS procedure consists of a mobile

identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, a registration type, and a security key set identifier for a NAS security context.

~~7~~6. The UE of claim ~~6~~5, wherein the instructions, when executed by ~~at least one memory and the computer program code are further configured, with~~ the at least one processor, further cause the UE to perform at least:

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

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

~~8~~7. The UE of claim 1, wherein:

the response comprises a security mode command message that indicates the NAS security algorithm and the security key set identifier; and

the subsequent NAS message comprises a security mode complete message having the NAS message container that contains the initial NAS message encrypted based on the NAS security algorithm.

~~9~~8. A network element of a mobility network comprising:

at least one processor; and

at least one memory storing instructions that, when executed by ~~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~~ during a first phase of the NAS procedure, the instructions, when executed by ~~at least one memory and the computer program code are configured, with~~ the at least one processor, cause the network element to perform at least:

~~receive,~~ receiving, from the UE, a first initial NAS message, the first initial NAS message containing ~~including~~ a first set of NAS protocol Information Elements (IEs) that includes only those NAS protocol IEs that are designated for security-related handling during the NAS procedure;

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~~ during a second phase of the NAS procedure, the instructions, when executed by ~~at least one memory and the computer program code are configured, with~~ the at least one processor, further cause the network element to perform:

~~receive,~~ receiving, 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 second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional NAS protocol IEs.

~~10~~9. The network element of claim ~~9~~8, wherein, ~~in~~ during the second phase of the NAS procedure, the second initial NAS message is encrypted within the NAS message container using the NAS security algorithm received ~~in~~ during the first phase of the NAS procedure.

~~11. The network element of claim 9, wherein, in the second phase of the NAS procedure, the second set of NAS protocol IEs includes the NAS protocol IEs in the first set of NAS protocol IEs and one or more additional NAS protocol IEs.~~

~~12~~10. The network element of claim ~~9~~8, wherein the first initial NAS message comprises at least a subset of the NAS protocol IEs that includes only those NAS protocol IEs that are designated for security-related handling during the NAS procedure, said subset of the NAS protocol IEs being encrypted by the UE using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

~~13~~11. The network element of claim ~~12~~10, wherein:

the first initial NAS message comprises a registration request message; and

the subset of NAS protocol IEs including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure consists of a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, a registration type, and a security key set identifier for a NAS security context.

~~14~~12. The network element of claim ~~9~~8, wherein:

the response comprises a security mode command message that indicates the NAS security algorithm and the security key set identifier; and

the subsequent NAS message comprises a security mode complete message having the NAS message container that contains the initial NAS message encrypted based on the NAS security algorithm.

~~15~~13. 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~~ during a first phase of the NAS procedure, said initiating comprises:

constructing a first initial NAS message, the first initial NAS message containing ~~including~~ a first set of NAS protocol Information Elements (IEs) including only 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 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~~ during 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, the second set of NAS protocol IEs including ~~which is different from~~ the first set of NAS protocol IEs and one or more additional NAS protocol IEs; and

sending the subsequent NAS message to the network element.

~~16~~14. 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~~ during a first phase of the NAS procedure, said causing comprises:

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

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~~ during 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, the second set of NAS protocol IEs including ~~which is different from~~ the first set of NAS protocol IEs and one or more additional IEs; and

sending the subsequent NAS message to the network element.

~~17~~15. User equipment (UE) comprising:

at least one processor; and

at least one memory storing instructions that, when executed by ~~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 by causing the UE to perform at least~~;~~

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

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

constructing a first initial NAS message, the first initial NAS message ~~including~~ containing an entire set of ~~first set of~~ NAS protocol Information Elements (IEs) for the NAS procedure; ~~that are designated for security-related handling,~~

constructing a second initial NAS message defining a same message type as the first initial NAS message and including the entire set of NAS protocol IEs for the NAS procedure;~~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~~

encapsulating the first initial NAS message in a NAS message container of the second initial NAS message; and

sending the ~~first~~ second initial NAS message to the network element.

~~18~~16. The UE of claim ~~17~~15, wherein the ~~second~~ first initial NAS message is encrypted within the NAS message container of the second initial NAS message using a NAS security algorithm associated with the NAS security context.

~~19~~17. The UE of claim ~~17~~15, wherein the entire ~~second~~ set of NAS protocol IEs for the NAS procedure includes ~~the~~ NAS protocol IEs designated for security-related handling~~information elements in the first set of NAS protocol IEs and one or more additional NAS protocol information elements~~.

~~20~~18. A network element of a mobility network comprising:

at least one processor; and

at least one memory storing instructions that, when executed by ~~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 participate in performing a Non-Access Stratum (NAS) procedure to establish a NAS communication session between user equipment (UE) and the network element by causing the network element to perform at least~~;~~

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

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

~~21~~19. The network element of claim ~~20~~18, wherein the ~~second~~ first initial NAS message is encrypted within the NAS message container of the second initial NAS message using a NAS security algorithm associated with the NAS security context.

~~22. The network element of claim 20, wherein the second set of NAS protocol IEs includes the NAS protocol information elements in the first set of NAS protocol IEs and one or more additional NAS protocol information elements.~~

~~23~~20. A method comprising:

causing user equipment (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 said causing comprises:

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

constructing a first initial NAS message, the first initial NAS message ~~including~~ containing an entire ~~first~~ set of NAS protocol Information Elements (IEs) ~~that are designated for security-related handling~~ for the NAS procedure, including one or more NAS protocol IEs designated for security-related handling;

constructing , the first initial NAS message further including a second initial NAS message containing a NAS message container and the entire set of NAS protocol IEs for the NAS procedure, including the one or more NAS protocol IEs designated for security-related handling;

encapsulating the first initial NAS message within the NAS message container of the 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 first second initial NAS message to the network element.

2421. A method comprising:

causing a network element to participate in performing a Non-Access Stratum (NAS) procedure to establish a NAS communication session between user equipment (UE) and the network element;

wherein said causing comprises:

receiving a first second initial NAS message from the UE, the first second initial NAS message including containing an entire first set of NAS protocol Information Elements (IEs) for establishment of the NAS communication session that are designated for security-related handling, the first second initial NAS message further including containing a second first initial NAS message encapsulated within a NAS message container IE of the second initial NAS message, the second first initial NAS message defining a same message type as the first second initial NAS message, the first initial NAS message containing the entire set of NAS protocol IEs for establishment of the NAS communication session and including a second set of NAS protocol IEs for the NAS procedure, which is different from the first set of NAS protocol IEs.

22. 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:

constructing a first initial Non-Access Stratum (NAS) message containing a first set of NAS protocol Information Elements (IEs) including only those NAS protocol IEs that are designated for security-related handling during a NAS procedure;

sending the first initial NAS message to a network element of a 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 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 and including a second set of NAS protocol IEs for a NAS procedure, the second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional NAS protocol IEs; and

sending the subsequent NAS message to the network element.

23. The UE of claim 22, wherein the second initial NAS message is encrypted within the NAS message container using the NAS security algorithm associated with the NAS security context.

24. The UE of claim 22, wherein the instructions, when executed by the at least one processor, further cause the UE to perform:

identifying, from an entire set of NAS protocol IEs, the first set of NAS protocol IEs including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure; and

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

25. The UE of claim 24, wherein the instructions, when executed by the at least one processor, further cause the UE to perform:

encrypting the first set of NAS protocol IEs in the first initial NAS message using a public key when the UE has the public key programmed on a UMTS Subscriber Identify Module (USIM) of the UE; and

sending the first initial NAS message to the network element without encrypting the first set of NAS protocol IEs in the first initial NAS message when the UE does not have the public key programmed on the USIM of the UE.

26. The UE of claim 24, wherein:

the first initial NAS message comprises a registration request message; and

the first set of NAS protocol IEs including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure consists of a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, a registration type, and a security key set identifier for a NAS security context.

27. The UE of claim 26, wherein the instructions, when executed by the at least one processor, further cause the UE to perform:

encrypting the first set 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 when the registration type does not indicate an emergency; and

sending the first initial NAS message to the network element without encrypting the first set of NAS protocol IEs in the first initial NAS message when the registration type indicates an emergency.

28. The UE of claim 22, wherein:

the response comprises a security mode command message that indicates the NAS security algorithm and the security key set identifier; and

the subsequent NAS message comprises a security mode complete message.

29. A network element of a mobility network comprising:

at least one processor; and

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

receiving, from a user equipment (UE), a first initial Non-Access Stratum (NAS) message containing a first set of NAS protocol Information Elements (IEs) that include only those NAS protocol IEs that are designated for security-related handling during a NAS procedure;

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;

sending, to the UE, the response to the first initial NAS message; 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 and including a second set of NAS protocol IEs for the NAS procedure, the second set of NAS protocol IEs including the first set of NAS protocol IEs and one or more additional NAS protocol IEs.

30. The network element of claim 29, wherein the second initial NAS message is encrypted within the NAS message container using the NAS security algorithm associated with the NAS security context.

31. The network element of claim 29, wherein the first set of NAS protocol IEs are encrypted using a public key of a Home Public Land Mobile Network (HPLMN) for the UE.

32. The network element of claim 31, wherein the first set of NAS protocol IEs are encrypted in the first initial NAS message using a public key when the UE has the public key programmed on a UMTS Subscriber Identify Module (USIM) of the UE, and wherein the first set of NAS protocol IEs are not encrypted in the first initial NAS message when the UE does not have the public key programmed on the USIM of the UE.

33. The network element of claim 31, wherein:

the first initial NAS message comprises a registration request message; and

the first set of NAS protocol IEs including only those NAS protocol IEs that are designated for security-related handling during the NAS procedure consists of a mobile identity for the UE, a UE security capability indicating one or more NAS security algorithms supported by the UE, a registration type, and a security key set identifier for a NAS security context.

34. The network element of claim 33, wherein the first set 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 when the registration type does not indicate an emergency, and wherein the first set of NAS protocol IEs are not encrypted in the first initial NAS message when the registration type indicates an emergency.

35. The network element of claim 29, wherein:

the response comprises a security mode command message that indicates the NAS security algorithm and the security key set identifier; and

the subsequent NAS message comprises a security mode complete message.

36. 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:

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

identifying, from among an entire set of NAS protocol Information Elements (IEs) used during the NAS procedure, a subset of NAS protocol IEs that include only 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;

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

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

receiving, in response to the first initial NAS message, from the network element, a response message that includes a NAS security algorithm and 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, the instructions, when executed by the at least one processor, cause the UE to perform:

inserting the entire set of NAS protocol IEs for the NAS procedure, including the subset of NAS protocol IEs that includes only those NAS protocol IEs that are designated for security-related handling during initiation of the NAS procedure, and one or more additional NAS protocol IEs, into a second initial NAS message, 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 a subsequent NAS message;

encrypting the NAS message container of the subsequent NAS message using the NAS security algorithm received in response to the first initial NAS message; and

sending the subsequent NAS message to the network element.

37. A network element of a mobility network comprising:

at least one processor; and

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

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

receiving, from the UE, a first initial NAS message containing a subset of NAS protocol Information Elements (IEs) selected from among an entire set of NAS protocol IEs, the subset of NAS protocol IEs including only 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;

constructing a response to the first initial NAS message that includes a NAS security algorithm and a 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, during a second phase of the NAS procedure, the instructions, when executed by the at least one processor, cause the network element to perform:

receiving, from the UE, a subsequent NAS message, the subsequent NAS message including a second initial NAS message encapsulated within a NAS message container IE 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 comprising the full set of NAS protocol IEs including the subset of NAS protocol IEs and one or more additional NAS protocol IEs.