## Claims

What is claimed is:

1. A method comprising:

in a home network of a communication system, wherein one or more cryptographic key pairs are provisioned for utilization by one or more of a plurality of subscribers of the home network to conceal subscriber identifiers provided to one or more access points in the communication system~~:~~:

provisioning one or more privacy managing entity identifiers for utilization by the subscribers when providing their concealed subscriber identifiers to the communication system, wherein each of the one or more privacy managing entity identifiers ~~identify~~ identifies ~~a given~~one privacy managing entity in the communication system configured to de-conceal a given concealed subscriber identifier,

receiving, at one of the one or more access points from user equipment, a request for authentication data for one of the plurality of subscribers, the request for authentication data comprising a concealed subscriber identifier and a privacy managing entity identifier, the privacy managing entity identifier identifying one of one or more privacy managing entities in the home network of the communication system configured to de-conceal the concealed subscriber identifier,

utilizing said one of the one or more privacy managing entities in the home network of the communication system identified by the privacy managing entity identifier in the request for authentication data to de-conceal the concealed subscriber identifier; and

obtaining, from one of a plurality of different instances of a user data repository, the authentication data for said one of the plurality of subscribers utilizing the de-concealed subscriber identifier, each of the plurality of different instances of the user data repository maintaining authentication data for a different subset of the plurality of subscribers of the home network of the communication system.

2. The method of claim 1, further comprising selecting ~~a~~ the one of the one or more privacy managing ~~entity~~ entities from the one or more privacy managing entities in the communication system based on ~~a~~ the ~~given~~ received privacy managing entity identifier ~~received from a given subscriber~~.

3. The method of claim 2, further comprising de-concealing the ~~given~~ received subscriber identifier at the selected privacy managing entity.

4. The method of claim 3, further comprising requesting subscriber authentication data concurrent with the privacy managing entity selecting step, wherein an authentication and security function of the communication system requests de-concealment of a given subscriber identifier concurrent with requesting authentication data for the given subscriber.

5. The method of claim 3, further comprising requesting subscriber authentication data following the de-concealing step, wherein an authentication and security function of the communication system requests de-concealment of a given subscriber identifier and, in response to receiving the de-concealed subscriber identifier, requests authentication data for the given subscriber.

6. The method of claim 1, wherein at least one of the one or more privacy managing entities is implemented in the communication system as a subscription identifier de-concealing function.

7. The method of claim 1, wherein the home network comprises multiple user data management instances.

8. The method of claim 7, wherein the multiple user data management instances comprise one or more user data management instances associated with one or more virtual network operators.

9. The method of claim 7, wherein a single privacy managing entity is used for the multiple user data management instances.

10. The method of claim 7, wherein multiple privacy managing entities are used for the multiple user data management instances.

11. An apparatus ~~comprising:~~

in a home network of a communication system, wherein one or more cryptographic key pairs are provisioned for utilization by subscribers of the home network to conceal subscriber identifiers provided to one or more access points in the communication system~~:~~, the apparatus comprising:

a processor operatively coupled to a memory and configured to:

provision one or more privacy managing entity identifiers for utilization by the subscribers when providing their concealed subscriber identifiers to the communication system, wherein each of the one or more privacy managing entity identifiers ~~identify~~ identifies ~~a given~~one privacy managing entity in the communication system configured to de-conceal a ~~given~~ concealed subscriber identifier,

receive, at one of the one or more access points from user equipment, a request for authentication data for one of the plurality of subscribers, the request for authentication data comprising a concealed subscriber identifier and a privacy managing entity identifier, the privacy managing entity identifier identifying one of one or more privacy managing entities in the home network of the communication system configured to de-conceal the concealed subscriber identifier,

utilize said one of the one or more privacy managing entities in the home network of the communication system identified by the privacy managing entity identifier in the request for authentication data to de-conceal the concealed subscriber identifier; and

obtain, from one of a plurality of different instances of a user data repository, the authentication data for said one of the plurality of subscribers utilizing the de-concealed subscriber identifier, each of the plurality of different instances of the user data repository maintaining authentication data for a different subset of the plurality of subscribers of the home network of the communication system.

12. A method comprising:

in user equipment, storing: ~~(i)~~ at least one public key associated with at least one cryptographic key pair, the at least one cryptographic key pair being provisioned by a home network of a communication system for use by the user equipment to conceal a subscriber identifier to be provided to one or more access points in the communication network; and ~~(ii)~~

at least one privacy managing entity identifier for utilization by the user equipment when providing a concealed subscriber identifier to the one or more access points in the communication system, wherein each of the one or more privacy managing entity identifiers identifies a ~~given~~ privacy managing entity of one or more privacy managing entities in the home network of the communication system configured to de-conceal the concealed subscriber identifier,

concealing the subscriber identifier utilizing one of the one or more public keys;

sending, from the user equipment to one of the one or more access points, a request for authentication data for one of a plurality of subscribers of the home network, the request for authentication data comprising the concealed subscriber identifier and one of the one or more privacy managing entity identifiers associated with one of the one or more privacy managing entities in the home network of the communication system; and

receiving, at the user equipment from said one of the one or more access points, the authentication data for said one of the plurality of subscribers, the authentication data being obtained from one of a plurality of different instances of a user data repository in the home network of the communication system, each of the plurality of different instances of the user data repository maintaining authentication data for a different subset of the plurality of subscribers of the home network or the communication system.

13. The method of claim 12, wherein the user equipment stores a key identifier that identifies the cryptographic key pair used by the user equipment to conceal the subscriber identifier, and further comprising sending the concealed subscriber identifier, the key identifier, and the privacy managing entity identifier to at least one access point in the communication system.

14. An apparatus comprising a processor operatively coupled to a memory and configured to perform the steps of claim 12.

15. An article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the steps of claim 12.