CLAIMS

1. A method, comprising:

forming a temporary privacy mask using a time-varying value and a privacy template;

encrypting a code value using the temporary privacy mask; and

transmitting the encrypted code value;

wherein the time-varying value is a UTC-based counter or a Message Integrity Code associated with the code value.

2. A method as in claim 1, comprising, as a preliminary step, receiving the privacy template.

3. A method as in claim 2, comprising receiving the privacy template from a network node.

4. A method as in claim 3, wherein the network node is a ProSe function node or a a ProSe Application Server.

5. A method as in one of claims 1 to 4, comprising forming the temporary privacy mask by applying a hash function to the time-varying value and the privacy template.

6. A method as in one of claims 1 to 5, wherein the code value is a ProSe code.

7. A method as in one of claims 1 to 6, comprising encrypting the code value using the temporary privacy mask by performing an XOR operation on the code value and the temporary privacy mask.

8. A method as in one of claims 1 to 7, comprising encrypting a part of the code value and leaving a part of the code value unencrypted.

9. A method as in one of claims 1 to 8, wherein the code value identifies an individual and the code is confidentiality protected using the privacy template specific to the individual or using the privacy template specific to a group.

10. A user equipment device, comprising a processor and a memory, the memory containing instructions executable by the processor, such that the user equipment device is operable to carry out a method according to any one of claims 1 to 9.

11. A method, comprising:

forming a temporary privacy mask using a time-varying value and a privacy template;

receiving an encrypted code value; and

decrypting the code value using the temporary privacy mask;

wherein the time-varying value is a UTC-based counter or a Message Integrity Code associated with the code value.

12. A method as in claim 11, comprising, as a preliminary step, receiving the privacy template.

13. A method as in claim 12, comprising receiving the privacy template from a network node.

14. A method as in claim 13, wherein the network node is a ProSe function node or a ProSe Application Server.

15. A method as in one of claims 11 to 14, comprising forming the temporary privacy mask by applying a hash function to the time-varying counter value and the privacy template.

16. A method as in one of claims 11 to 15, wherein the code value is a ProSe code.

17. A method as in one of claims 11 to 16, comprising decrypting the code value using the temporary privacy mask by performing an XOR operation on the encrypted code value and the temporary privacy mask.

18. A method as in one of claims 11 to 17, further comprising testing whether the decrypted code value is recognized by comparing at least a part of the decrypted code value with a stored code value.

19. A method as in one of claims 11 to 18, wherein the code value identifies an individual and the code is confidentiality protected using the privacy template specific to the individual or using the privacy template specific to a group.

20. A user equipment device, comprising a processor and a memory, the memory containing instructions executable by the processor, such that the user equipment device is operable to carry out a method according to any one of claims 11 to 19.

21. A computer program configured, when run on a computer, to carry out a method according to any one of claims 1 to 9 or 11 to 19.

22. A computer program product comprising computer readable medium and a computer program according to claim 21 stored on the computer readable medium.