CLAIMS

1. A method in a client terminal (100, 400) for enabling safe communication with a web server (106, 402), the method comprising:

- obtaining (202) a web page from the web server in a session with the web server,

- determining (204) a set of context parameters, P1,...Pn, pertaining to said session ~~and/or~~with the web serverpage~~,~~

- creating (206) a context specific key, Ks_NAF', based on said context parameters, and

- using (208) the created context specific key Ks_NAF' for verification of the client in the web server if a context specific key determined in the web server matches the context specific key created by the client terminal.

2. A method according to claim 1, wherein the created context specific key Ks_NAF' is indicated in a login request to the web server.

3. A method according to claim 1 or 2, wherein said context parameters include at least one of: a path component of a Universal Resource Locator (URL) of said web page, a current HTTP session identity of said session, and a current Transport Layer Security (TLS) / Secure Socket Layer (SSL) session identity of said session.

4. A method according to any of claims 1-3, wherein the context specific key Ks_NAF' is created by applying a predefined Key Derivation Function, KDF, to said context parameters, the Key Derivation Function being known to the web server.

5. A method according to claim 4, wherein an aggregated parameter, S, is created based on the context parameters P1,...Pn in a predetermined manner, and the Key Derivation Function is applied using as input said aggregated parameter S and an application specific key, Ks_NAF, such that

Ks_NAF' = KDF(Ks_NAF, S(P1,...Pn)).

6. A method according to claim 5, wherein the application specific key Ks_NAF has been derived from a master key, Ks, obtained from a Bootstrapping Service Function, BSF.

7. A method according to any of claims 1-6, wherein the context parameters are determined in communication with the web server having a Network Application Function, NAF.

8. A client terminal (400) configured to enable safe communication with a web server (402), the client terminal comprising:

- a receiving module (400a) adapted to obtain a web page from the web server in a session with the web server,

- a key creating module (400b) adapted to determine a set of context parameters, P1,...Pn, pertaining to said session ~~and/or~~with the web serverpage, and to create a context specific key, Ks_NAF', based on said context parameters, and

- a sending module (400c) adapted to send a login request indicating the created context specific key Ks_NAF' to the web server to enable verification of the client if a context specific key determined in the web server matches the context specific key created by the client terminal.

9. A client terminal according to claim 8, wherein the key creating module (400b) is further adapted to create the context specific key Ks_NAF' by applying a predefined Key Derivation Function, KDF, to said context parameters, the Key Derivation Function being known to the web server.

10. A client terminal according to claim 9, wherein the key creating module (400b) is further adapted to create an aggregated parameter, S, based on the context parameters P1,...Pn in a predetermined manner, and the Key Derivation Function is applied using as input said aggregated parameter S and an application specific key, Ks_NAF, such that

Ks_NAF' = KDF(Ks_NAF, S(P1,...Pn)).

11. A client terminal according to any of claims 8-10, wherein the key creating module (400b) is further adapted to determine the context parameters in communication with the web server having a Network Application Function, NAF.

12. A method in a web server (106, 402) for enabling safe communication with a client terminal (100, 400), the method comprising:

- sending (302) a web page to the client terminal in a session with the client terminal,

- receiving (304) a login request from the client terminal indicating a context specific key, Ks_NAF', created by the client terminal,

- determining (306) a set of context parameters, P1,...Pn, pertaining to said session ~~and/or~~with the client terminal~~web page~~,

- determining (308) a context specific key, Ks_NAF', based on said context parameters, and

- verifying (314) the client if the context specific key determined in the web server matches the context specific key created by the client terminal.

13. A method according to claim 12, wherein said context parameters include at least one of: a path component of a Universal Resource Locator (URL) of said web page, a current HTTP session identity of said session, and a current Transport Layer Security (TLS) / Secure Socket Layer (SSL) session identity of said session.

14. A method according to claim 12 or 13, wherein the context specific key Ks_NAF' is created by applying a predefined Key Derivation Function, KDF, to said context parameters, the Key Derivation Function being known to the client terminal.

15. A method according to claim 14, wherein an aggregated parameter, S, is created based on the context parameters P1,...Pn in a predetermined manner, and the Key Derivation Function is applied using as input said aggregated parameter S and an application specific key, Ks_NAF, such that

Ks_NAF' = KDF(Ks_NAF, S(P1,...Pn)).

16. A method according to claim 15, wherein the application specific key Ks_NAF is obtained from a Bootstrapping Service Function, BSF, associated with the client terminal.

17. A web server (402) configured to enable safe communication with a client terminal (400), the web server comprising:

- a sending module (402a) adapted to send a web page to the client terminal in a session with the client terminal,

- a receiving module (402b) adapted to receive a login request from the client terminal indicating a context specific key, Ks_NAF', created by the client terminal, and

- a verification module (402c) adapted to determine a set of context parameters, P1,...Pn, pertaining to said session ~~and/or~~with the client terminal~~web page~~, determine a context specific key, Ks_NAF', based on said context parameters, and to verify the client if the context specific key determined in the web server matches the context specific key created by the client terminal.

18. A web server according to claim 17, wherein the verification module (402c) is further adapted to create the context specific key Ks_NAF' by applying a predefined Key Derivation Function, KDF, to said context parameters, the Key Derivation Function being known to the client terminal.

19. A web server according to claim 18, wherein the verification module (402c) is further adapted to create an aggregated parameter, S, based on the context parameters P1,...Pn in a predetermined manner, and to apply the Key

Derivation Function using as input said aggregated parameter S and an application specific key, Ks_NAF, such that

Ks_NAF' = KDF(Ks_NAF, S(P1,...Pn)).

20. A web server according to claim 19, wherein the verification module (402c) is further adapted to obtain the application specific key Ks_NAF from a Bootstrapping Service Function, BSF, associated with the client terminal.