

CLAIMS

1. In a client server environment a method of securely storing data generated at a first location for use on a client device at a second location; the first location separate and remote from the second location; the improvement comprising said method comprising

for a first use of the method of securely storing the data at the second location by a user, executing the following steps:

the user initiates a secure connection to a first device in the form of a server;

a client device of the user at a second location is logged onto a secure user account;

subsequently the server at the first location supplies a form for use by the user to format a data to be secured;

the user fills out the form with the data to be secured;

the user then opts to store the data securely on their client device at the second location;

the server at the first location then retrieves the data from the second location during an unencrypted window period and processes it;

subsequently an encryption key is generated by the server at the first location and the key is linked to the secure user account;

the key is then used to encrypt the data to be protected and the resulting encrypted data is stored during an encrypted window period on the client device of the user at the second location; the server then deleting all of the data and the encrypted data on the server; the new encryption key remaining stored only on the server;

and for a second use of the method, executing the following steps:

the user starts a secure connection and the server then establishes a secure connection using the secure user account;

during the course of second use the server at the first location presents the user with a form to collect the encrypted data that the user has opted to encrypt and securely store on their client device at the second location in the past;

the user is then given the option and chooses to use the encrypted data already stored on the client device at the second location;

the server at the first location retrieves the encrypted data from the client device at the second location;

the server then retrieves the encryption key from the associated secure user account and the data is decrypted on the server to memory and made available to the user and the data is processed as needed;

after use of the data by the user subsequently the server generates a new encryption key which is used to re-encrypt the data so that it can be stored again on the client device at the second location;

the new encryption key is then stored with the secure user account on the server at the first location in the anticipation of future decryption and use;

the server then deleting all of the data and the encrypted data on the server; the new encryption key remaining stored only on the server during the encrypted window period and referenced against the user name account; and

wherein the client device is programmed to execute a Web enabled application which has a storage capability; and wherein the encrypted data element is stored on the client device utilising the storage capability of the Web enabled application; and

wherein the Web enabled application is a Web browser; and wherein the web browser executes HTML 5 including the HTML 5 local storage function.

2. The method of claim 1 wherein the data is generated at the second location.

3. The method of claim 1 or claim 2 wherein in the second use the data is used on the client device at the second location.

4. The method of claim 1, 2 or 3 wherein the client device stores the encrypted data in local storage of a browser or web enabled applications for future retrieval.

5. The method of claim 1 or claim 2 or claim 3 wherein the first location is constituted as a web enabled server.

6. The method of any previous claim wherein the step of encryption of the data after use is performed including the step of generating a new encryption key.

7. The method of any previous claim wherein the data is amended during use.

8. The method of any previous claim wherein an encryption key for the encrypted data is generated at the first location and stored at the first location or within its network environment.

9. The method of any previous claim wherein the first location is constituted by a server device and the key is

stored on the server device or within its network environment.

10. A method of isolation from its encryption key of encrypted data stored on a client device; the improvement comprising said method comprising
storing the encryption key referenced against a username account/ user login-data for the client device on a separate device; retrieving the data by transferring the encrypted data to the separate device and upon authentication of the user login/username account decrypting the encrypted data using the encryption key for use of the decrypted data during an unencrypted window period; at the end of the unencrypted window period the separate device re-encrypting the data with a new encryption key to form re-encrypted data; storing the re-encrypted data on the client device;
then deleting all of the data and the encrypted data on the separate device thereby terminating the unencrypted window period; the encryption key remaining stored only on the separate device; and
wherein the client device is programmed to execute a Web enabled application which has a storage capability; and
wherein the encrypted data element is stored on the client device utilising the storage capability of the Web enabled application; and
wherein the Web enabled application is a Web browser; and
wherein the web browser executes HTML 5 including the HTML 5 local storage function.

11. The method of claim 10 wherein the separate device is a Web server.

12. The method of claim 10 or 11 wherein the user login is a username and password.

13. The method of any one of claims 10 to 12 wherein in a client server environment during a secured non-use window data is stored securely on the client device as encrypted data requiring decryption by decrypting the encrypted data and wherein the encryption key is not stored on the client device.