

Claims

1. An encryption system (10) arranged to receive, for each of a plurality of data fields, content of the data field and a designation of encryption type, the encryption system (10) being arranged to apply the encryption type to the content of the
5 respective data field and associate metadata on the encryption type with the encrypted content, characterised in that the encryption system (10) further comprises a data repository (30) to receive an access condition for one or more of said data fields, the data repository being arranged to receive different access conditions for different content of a respective data field, the data repository being
10 arranged to receive key data associated with said access condition, the encryption system (10) being arranged to access the data repository (30) and determine whether the respective access condition is met by the accessor at the time of attempted access to the encrypted content and to permit use of said key data upon said respective access condition for the content being satisfied.
15
2. The encryption system (10) of claim 1, further comprising a further data repository to store the encrypted content, the further data repository being remote of the data repository.
- 20 3. The encryption system (10) of claim 1 or 2, wherein at least a subset of the data fields store content on users, the encryption system (10) storing content in the data fields on plural users and the access condition for a data field being dependent on the user.
- 25 4. The encryption system (10) of claim 1 or 2, wherein at least a subset of the data fields store content on users and the content is provided by a party different to the user, the encryption system (10) storing content in the data fields from plural parties providing the content and the access condition being dependent on the party providing the content.

30

5. The encryption system (10) of claim 3, further comprising a user interface control associated with the data field for receiving a designation of encryption type from the user.

5

6. The encryption system (10) of claim 4, a user interface control associated with the data field for receiving a designation of encryption type from the party providing the content.

10 7. The encryption system (10) of any preceding claim, further arranged to receive content for on a data field without designation of encryption type, the encryption system being arranged to cause storage of the content in the further data repository without encryption.

15 8. A decryption system (100) for providing access to remotely stored data items, (120a-c) each of the data items (120a-c) being independently accessible, wherein at least a subset of the remotely stored data items (120a-b) are encrypted, characterised in that each encrypted data item (120a-b) has an associated access condition (130a-b) specifying conditions to be met for encryption key data to be
20 accessible for decrypting the encrypted data item, the access conditions (130a-b) being stored in a data repository (110) and the data repository (110) being arranged to receive different access conditions for different content of a respective data field, wherein upon a client requesting access to a remotely stored data item, the decryption system (100) being arranged provide non-encrypted data items and for
25 encrypted data items, access the data repository (110) to determine the access condition and provide a decrypted data item if the associated access condition is met.

9. The decryption system of claim 8, wherein an access condition comprises
30 the client requesting access being at a physical location or within a physical region,

or at or within one of a number of predetermined physical locations or physical regions, the decryption system being configured to access a geolocation or GPS system to determine the client's physical location and determine if the access condition is met using data from the geolocation or GPS system.

5

10. An encryption method comprising:

receiving at an encryption system (10), for each of a plurality of data fields, content of the data field and a designation of encryption type;

applying the encryption type to the content of the respective data field and

10 associating metadata on the encryption type with the encrypted content;

characterised by:

receiving, at a data repository (30) of the encryption system (10), an access condition for one or more of said data fields, the access condition being dependent on the content, the data repository being arranged to receive different access

15 conditions for different content of a respective data field,

receiving, at the data repository (30), key data associated with said access condition;

accessing the data repository (30) by the encryption system (10) and determining whether the respective access condition is met by the accessor at the time of

20 attempted access to the encrypted content; and,

permitting use of said key data upon said respective access condition for the content being satisfied.

11. The method of claim 10, wherein at least a subset of the data fields store
25 content on users and the content is provided by a party different to the user, the method further comprising storing content in the data fields from plural parties providing the content, the access condition being dependent on the party providing the content.

12. The method of claim 11, further comprising receiving, from a user interface control associated with the data field, a designation of encryption type from the party providing the content.

5 13. The method of claim 10, 11 or 12, further comprising causing storage of the content in the data repository without encryption upon receiving content for on a data field without designation of encryption type.

10 14. A decryption method for providing access to remotely stored data items, each of the data items being independently accessible, wherein at least a subset of the remotely stored data items (120a-b) are encrypted, characterised in that each encrypted data item (120a-b) has an associated access condition (130a-b) specifying conditions to be met for encryption key data to be accessible for decrypting the encrypted data item, the access conditions (130a-b) being stored in
15 a data repository (110) and the data repository being arranged to receive different access conditions for different content of a respective data field, the method comprising:

receiving a request from a client to access one of the remotely stored data items;
upon the requested data item being non-encrypted, providing access to the data
20 item;
upon the data item being encrypted, determining the access condition associated with the data item;
determining if the access condition is met by the client and, upon the access condition being met, providing access to the decrypted data item.

25 15. The decryption method of any claim 14, wherein an access condition comprises the client requesting access being at a physical location or within a physical region, or at or within one of a number of predetermined physical locations or physical regions, the method further comprising accessing a geolocation or GPS

system to determine the client's physical location and determining if the access condition is met using data from the geolocation or GPS system.