Claims

1. A system for providing secure access to a digital asset, the system comprising:

a first computing device operating in an offline environment, wherein the first computing device is configured to generate an access control object comprising at least an access control identifier associated with an access policy of a client; and

a second computing device operating in an online environment, wherein the second computing device is configured to generate at least one vault object associated with the access control object, the vault object comprising:

a first dataset comprising at least the access control identifier; and

a vault identifier, wherein the vault identifier is calculated in dependence on the first dataset;

wherein the first computing device is further configured to generate at least one digital asset object associated with the vault object, the digital asset object comprising a digital asset and the vault identifier.

2. A system according to claim 1, wherein the second computing device is further configured to calculate the vault identifier by inputting the first dataset to a hash function.

3. A system according to claims 1 or 2, wherein the first dataset further comprises a client identifier uniquely identifying the client, wherein the access control object optionally further comprises the client identifier.

4. A system according to any preceding claim, wherein the first computing device is configured to integrity protect the access control object and/or the digital asset object using one or more integrity cryptographic keys stored in the offline environment.

5. A system according to claim 4, wherein the first computing device is configured to apply a digital signature or hash-based message authentication code (HMAC) to the access control object.

6. A system according to claims 4 or 5, wherein the first computing device is further configured to encrypt the digital asset using an encryption key stored in the offline environment, wherein the encryption is optionally an authenticated encryption process.

7. A system according to any preceding claim, wherein the digital asset comprises a cryptographic key for digitally signing cryptographic operations.

8. A system according to any preceding claim, wherein the access control object further comprises the access policy associated with the client, wherein the access policy is indicative of one or more authorisation checks for using a digital asset associated with the client.

9. A system according to any preceding claim, wherein the second computing device is configured to generate a plurality of vault objects associated with the access control object.

10. A system according to any preceding claim, wherein the first computing device is configured to generate a plurality of digital asset objects associated with the vault object.

11. A system according to any preceding claim, wherein the first computing device is configured to authorise access to the digital asset contained in the digital asset object in dependence on the first dataset contained in the vault object.

12. A system according to any preceding claim, wherein the first computing device is further configured to:

receive a request for access to the digital asset, the request comprising data indicative of a result of one or more executed authorisation checks;

receive the vault object;

calculate a verification identifier based on the first dataset of the received vault object;

compare the verification identifier to the vault identifier of the digital asset object;

verify that the vault object is associated with the access control object and digital asset object based on the comparison of the verification identifier and the vault identifier; and

authorise access to the digital asset in dependence on the verifying.

13. A system according to claim 12, wherein the vault object is verified as being associated with the access control object and the digital asset object if the verification identifier matches the vault identifier.

14. A system according to claims 12 or 13, wherein the first computing device is further configured to process the result of the one or more executed authorisation

checks based on an access policy defined by the access control object, wherein the access policy is indicative of one or more authorisation checks for using the digital asset.

15. A system according to any of claims 11 to 14, wherein the first computing device is further configured to evaluate the integrity of the access control object and digital asset object using one or more integrity cryptographic key stored in the offline environment.

16. A system according to any of claims 11 to 15, wherein the first computing device is further configured to verify that the first dataset of the received vault object comprises the access control identifier associated with the access policy.

17. A system according to any of claims 11 to 16, wherein the verification identifier is calculated by inputting the first dataset of the received vault object to a hash function.

18. A system according to claims 10 to 17, wherein the digital asset comprises a cryptographic key for digitally signing cryptographic operations, and wherein the first computing device is further configured to digitally sign a cryptographic operation using the cryptographic key of the digital asset object.

19. A computer-implemented method of generating data objects for use in controlling access to a digital asset, the method comprising:

generating an access control object comprising at least an access control identifier associated with an access policy of a client, the access control object being generated and integrity protected within a secure offline environment;

generating at least one vault object associated with the access control object, the vault object comprising:

a first dataset comprising at least the access control identifier; and

a vault identifier associated therewith, wherein the vault identifier is calculated in dependence on the first dataset, the vault object being generated within an online environment; and

generating at least one digital asset object associated with the vault object, the digital asset object comprising at least one digital asset and the vault identifier, the digital asset object being generated and integrity protected within the secure offline environment.

20. A computer program configured to perform the method of claim 19 when executed on one or more processors.