

Other previous attempts to solve this problem include so-called “key escrow” systems. A key escrow system is a system in which the keys that are required to decrypt some encrypted data are held in escrow so that an authorised or designated third party may gain access to those keys under certain conditions. Verifying that any such conditions are met poses several problems. Existing key escrow systems rely on the correct functioning of some social linkage, such as a court order together with its verification and technical enforcement, or a connected individual or institutional body charged with controlling access to the key. As such, these systems still require an element of socially or institutionally founded trust in order to function correctly. The limitations and drawbacks of existing key escrow mechanisms are described in more detail in “*The risks of key recovery, key escrow, and trusted third-party encryption*” Hal Abelson et al. (1997), World Wide Web J. 2, 3 (June 1997), 241-257.

There is a need for a cryptographic protocol that enables authorised third parties to access encrypted information in a way that does not compromise the security of the underlying information and that provides the owner of the encrypted information with an inevitable, overt, persistent and secure record that the information has been accessed by the authorised third party so that illegal, unwarranted, inappropriate or otherwise unauthorised access can be dealt with through the courts or other social channels.

Summary of the Invention

According to a first aspect of the present invention, a system for providing access to a designated third party system to a secret is provided. The system comprises a plurality of trustee systems, and each trustee system is configured to receive a secret share of the secret from a first party system and store the secret share. Either the secret or the secret share is encrypted such that only a designated third party system can access the secret. Each trustee system is also configured to monitor published requests for the secret shares, validate that a given request for the secret shares was made by the designated third party system and, if the validation is successful, publish the secret share in response to the validated request for the secret shares, wherein the secret shares are published by the trustee system to a first ledger, and wherein the requests for the secret shares are published to the first ledger, or to a second ledger.

Each published request for the secret shares may comprise a validation token and an encrypted validation token, and each trustee system may be further configured to receive a second key of a validation key pair from the first party system along with the secret share and store the second key of the validation key pair, validate that the request for the secret

The third party system may be further configured to decrypt the encrypted secret or secret shares using the private key of the key pair associated with the third party system or, when the secret is encrypted with second key of the validation key pair, decrypt the encrypted secret or secret shares with the first validation key of the validation key pair.

5

When the secret is a first key of an object key pair, the third party system is further configured to receive the encrypted data from the first party system, and decrypt the encrypted data using the decrypted second object key of the object key pair.

10 The third party system may be further configured to validate the secret shares published in response to the request for the secret shares by comparing the decrypted second validation token published with the secret shares to a local copy of the second validation token, such that when the decrypted second validation token matches the local copy of the second validation token, the third party system retrieves the associated secret share.

15

Each trustee system may be further configured to generate a second validation token, encrypt the second validation token using the second validation key of the validation key pair to generate an encrypted second validation token, and publish the second validation token and the encrypted second validation token with the secret share. In this case, the third party system is further configured to validate the secret shares published in response to the request for the secret shares by decrypting the encrypted second validation token using the first validation key of the validation key pair, comparing the decrypted second validation token with the second validation token and retrieving the associated secret share when the decrypted second validation token matches the second validation token.

20

25

According to a second aspect of the invention, a method for providing to a designated third party system access to a secret is provided. The method comprises receiving, at a trustee system, a secret share of the secret from a first party system and storing the secret share, wherein the secret or the secret share is encrypted such that only a designated third party system can access the secret, monitoring published requests for the secret shares, validating that a request for the secret shares was made by the designated third party system, and if the validation is successful, publishing the secret share in response to the validated request for the secret shares, wherein the secret shares are published by the trustee system to a first ledger, and wherein the requests for the secret shares are published to the first ledger, or to a second ledger.

30

35

It will be appreciated that the method may also include steps corresponding to all of the claimed features of the trustee, first party and third party systems set out above.