CLAIMS

1. A method for distributing encrypted data objects performed by a sender computer of a sender, comprising:

encrypting, by ~~one or more processors~~a processor, data based at least in part on a session key to generate encrypted data;

encrypting, by the ~~one or more processors~~processor, the session key based at least in part on a sender key to generate an encrypted session key,

the sender key previously obtained from a key management system (KMS);

transmitting, by the ~~one or more processors~~processor, a request to the KMS for an encrypted sender key index, the request comprising an index of the sender key and an index of each of ~~one or more additional keys;~~a plurality of additional keys, each of the plurality of additional keys is accessible by a defined group of users,

~~receiving, by the one or more processors, the encrypted~~ wherein the sender key index is encrypted by the KMS using a combined key derived from a combination of the ~~KMS~~plurality of additional keys obtained based on the indices of the plurality of additional keys;

receiving, by the processor, the encrypted sender key index ~~generated by~~from the KMS ~~based at least in part on the sender key and the one or more additional keys~~;

generating, by the ~~one or more processors~~processor, an object that includes the encrypted data, the encrypted session key, the index of each of the ~~one or more~~plurality of additional keys, and the encrypted sender key index,

wherein access to the data via the object is controlled based at least in part on whether a receiver has access to the sender key and to ~~the one or more additional keys~~each of the plurality of additional keys, wherein access to each of the plurality of additional keys is based on user metadata indicating that the receiver is being defined in each group of users associated with each of the plurality of additional keys, wherein a user metadata is updated based on a change in a user's status.

2. The method of claim 1, wherein access to the data via the object is further controlled based at least in part on whether the sender key and the ~~one or more~~plurality of additional keys are ~~–~~valid.

3. The method of claim 2, further comprising preventing the receiver from accessing the data via the object, the preventing comprising transmitting a request to the KMS to invalidate the sender key.

4. The method of claim 2, further comprising preventing the receiver from accessing the data via the object, the preventing comprising transmitting a request to the KMS to invalidate at least one of the ~~one or more~~plurality of additional keys.

5. The method of claim 1, wherein access to the data via the object is modified in response to the KMS adding or removing the receiver from a list of users having access to the sender key.

6. The method of claim 1, wherein access to the data via the object is modified in response to the KMS adding or removing the receiver from a list of users having access to an additional key of the ~~one or more~~plurality of additional keys.

7. The method of ~~any preceding~~ claim 1, further comprising transmitting the object to the receiver.

8. The method of claim 7, wherein the transmitting is via a network.

9. A sending system of a sender for distributing encrypted data objects comprising:

~~———~~a memory for storing computer-readable instructions and one or more processors for executing ~~computer-readable instructions,~~ the computer-readable instructions, the computer-readable instructions controlling the one or more processors to perform operations comprising:

~~———~~encrypting data based at least in part on a session key to generate encrypted data;

~~———~~encrypting the session key based at least in part on a sender key to generate an encrypted session key, the sender key previously obtained from a key management system (KMS);

transmitting a request to the KMS for an encrypted sender key index,

the request comprising an index of the sender key and an index of each of ~~one or more~~ a plurality of additional keys~~;~~, each of the plurality of additional keys is accessible by a defined group of users,

~~———~~wherein the sender key index is encrypted by the KMS using a combined key derived from a combination of the plurality of additional keys;

receiving the encrypted sender key index from the KMS~~, the encrypted sender key index generated by the KMS based at least in part on the sender key~~ ; and ~~the one or more additional keys; and~~

~~———~~generating an object that includes the encrypted data, the encrypted session key, the index of each of the ~~one or more~~plurality of additional keys, and the encrypted sender key index,

wherein access to the data via the object is controlled based at least in part on whether a receiver has access to the sender key and to ~~the one or more additional keys~~each of the plurality of additional keys, wherein access to each of the plurality of additional keys is based on user metadata indicating that the receiver is being defined in each group of users associated with each of the plurality of additional keys, wherein a user metadata is updated based on a change in a user's status.

10. ~~———~~ The system of claim 9, wherein access to the data via the object is further controlled based at least in part on whether the sender key and the ~~one or more~~plurality of additional keys are valid.

11. The system of claim 10, wherein the operations further comprise preventing the receiver from accessing the data via the object, the preventing comprising transmitting a request to the KMS to invalidate the sender key.

12. The system of claim 10, wherein the operations further comprise preventing the receiver from accessing the data via the object, the preventing comprising transmitting a request to the KMS to invalidate at least one of the ~~one or more~~plurality of additional keys.

13. The system of claim 9, wherein access to the data via the object is modified in response to the KMS adding or removing the receiver from a list of users having access to the sender key.

14. The system of claim 9, wherein access to the data via the object is modified in response to the KMS adding or removing the receiver from a list of users having access to an additional key of the ~~one or more~~plurality of additional keys.

15. A sender computer program product of a sender for distributing encrypted data objects, comprising a computer-readable storage medium having program instructions embodied therewith, the program instructions executable by ~~one or more processors~~a processor to cause the ~~one or more processors~~processor to perform operations comprising:

~~———~~encrypting data based at least in part on a session key to generate encrypted data;

~~———~~encrypting the session key based at least in part on a sender key to generate an encrypted session key, the sender key previously obtained from a key management system (KMS);

transmitting a request to the KMS for an encrypted sender key index,

the request comprising an index of the sender key and an index of each of ~~one or more~~a plurality of additional keys~~;~~,

~~———~~each of the plurality of additional keys is accessible by a defined group of users,

wherein the sender key index is encrypted by the KMS using a combined key derived from a combination of the plurality of additional keys;

receiving the encrypted sender key index from the KMS~~, the encrypted sender key index generated by the KMS based at least in part on the sender key~~ ; and ~~the one or more additional keys; and~~

~~———~~generating an object that includes the encrypted data, the encrypted session key, the index of each of the ~~one or more~~plurality of additional keys, and the encrypted sender key index, wherein access to the data via the object is controlled based at least in part on whether a receiver has access to the sender key and to each of the ~~one or more~~plurality of additional keys~~.~~,

wherein access to each of the plurality of additional keys is based on user metadata indicating that the receiver is being defined in each group of users associated with each of the plurality of additional keys, wherein a user metadata is updated based on a change in a user's status.

16. A method for decrypting data objects performed by a receiver computer of a receiver comprising:

~~———~~receiving from a sender, by ~~one or more processors, an~~a processor, a data object that includes encrypted data, an encrypted session key, an index of each of ~~one or more~~a plurality of additional keys, and an encrypted sender key index~~;~~, each of the plurality of additional keys is accessible by a defined group of users;

~~———~~transmitting, by the ~~one or more processors~~processor, a request for a sender key corresponding to the encrypted sender key index to a key management system (KMS), ~~the request from a requestor and the request comprising the encrypted sender key index and the index of each of the one or more additional keys; and~~

~~———~~the request from the receiver comprising the encrypted sender key index and the index of each of the plurality of additional keys,

wherein the KMS, in response to the request, obtains each of the plurality of additional keys based on each respective index, decrypts the encrypted sender key index using a combined key derived from a combination of the obtained plurality of additional keys, and transmitting the sender key to the receiver based on the sender key index; and

in response to receiving the sender key from the KMS:

~~———~~decrypting the encrypted session key based at least in part on the sender key to generate a session key; and

~~———~~decrypting the encrypted data based at least in part on the session key to generate unencrypted data, wherein the sender key is sent to the ~~requestor~~receiver by the KMS in response to a determination by the KMS that the ~~requestor~~receiver has access to the sender key and to each of the ~~one or more~~plurality of additional keys, wherein access to each of the plurality of additional keys is based on user metadata indicating that the receiver is being defined in each group of users associated with each of the plurality of additional keys, wherein a user metadata is updated based on a change in a user's status.

17. The method of claim 16, further comprising receiving an error message from the KMS in response to a determination by the KMS that the ~~requestor~~receiver does not have access to the sender key.

18. The method of claim 17, wherein it is determined that the ~~requestor~~receiver does not have access to the sender key when the sender key is invalid.

19. The method of claim 16, further comprising receiving an error message from the KMS in response to a determination by the KMS that the ~~requestor~~receiver does not have access to all of the ~~at least one or more~~plurality of additional keys.

20. The method of claim 19, wherein it is determined that the ~~requestor~~receiver does not have access to all of the ~~one or more~~plurality of additional keys when at least one of the ~~one or more~~plurality of additional keys is invalid.

~~21. A method comprising:~~

~~receiving, by one or more processors, a request from a requestor for a sender key, the request comprising an encrypted sender key index and an index of each of one or more additional keys;~~

~~determining whether the requestor has access to one or more additional keys identified by the index of each of the one or more additional keys; and~~

~~in response to determining that the requestor has access to the one or more additional keys:~~

~~decrypting the encrypted sender key index to generate a sender key index;~~

~~locating the sender key based at least in part on the sender key index;~~

~~determining whether the requestor has access to the sender key; and~~

~~transmitting the sender key to the requestor based on determining that the requestor has access to the sender key.~~

~~22. The method of claim 21, further comprising generating the encrypted sender key index based at least in part on the sender key index and the index of each of the one or more additional keys.~~

~~23. The method of claim 22, wherein the generating comprises:~~

~~locating the one or more additional keys based at least in part on an index of each of the one or more additional keys;~~

~~combining the one or more additional keys into a combined additional key; and~~

~~encrypting the sender key index based at least in part on the combined additional key.~~