CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for providing data storage services, comprising:

obtaining, from a customer device associated with the computing resource service provider, information related to a policy associated with a cryptography service, the policy including a limitation on cryptographic information generated by a cryptography service of the computing resource service provider;

processing the policy to cause the cryptography service to impose the limitation on the cryptographic information; and

causing the cryptography service to use, subject to the limitation, the cryptographic information to encrypt or decrypt the data such that the cryptographic information is only accessible to the cryptography service, the encrypting or decrypting the data including enabling the cryptography service, based at least in part on the limitation, to select the cryptographic information from a larger set of cryptographic information stored by the cryptography service; and

providing an outcome of the use of the cryptographic information.

2. The computer-implemented method of claim 1, wherein causing the cryptography service to encrypt or decrypt the data is further subject to valid proof information that enables the cryptography service to verify authenticity of an obtained request to encrypt or decrypt the data.

3. The computer-implemented method of claim 1, wherein the limitation includes a limitation on authorized requestors capable of causing the cryptography service to perform cryptographic operations using the cryptographic information.

4. The computer-implemented method of claim 1, wherein the limitation includes a limitation on a number of uses of the cryptographic information.

5. The computer-implemented method of claim 1, wherein the limitation includes a limitation on using the cryptographic information to decrypt or encrypt one or more types of data.

6. A computer system, comprising:

one or more processors; and

memory storing instructions executable by the one or more processors to cause the computer system to implement at least:

a cryptography service configured to at least:

process a policy related to a plurality of keys, the policy including one or more limitations on using the plurality of keys;

store the plurality of keys such that the plurality of keys are inaccessible to a service different from the cryptography service;

detect a pending request to process data;

select, based at least in part on a key identifier provided by the service different from the cryptography service and provided subject to the one or more limitations, a key from the plurality of keys;

process the data with the selected key to perform one or more cryptographic operations associated with the pending request; and

provide, to a requestor associated with the request, an outcome associated with the use of the selected key.

7. The computer system of claim 6, wherein detecting the request includes obtaining, from the service, a notification and proof of the request.

8. The computer system of claim 6, wherein:

the computer system is operated by a computing resource service provider;

the request is generated by a customer device of a plurality of customer devices of the computing resource provider; and

each key of the plurality of keys is associated with a different corresponding customer of the plurality of customer devices.

9. The computer system of claim 6, wherein the cryptography service is further configured to verify, against the policy, that the pending request is authorized.

10. The computer system of claim 6, further comprising a metering service configured to obtain output of the cryptography service and generate accounting records based at least in part on the policy.

11. The computer system of claim 6, wherein the cryptography service is further configured to enforce at least one or more policies for each of at least a subset of the plurality of keys.

12. The computer system of claim 11, wherein:

the computer system is operated by a computing resource service provider;

each key of the plurality of keys corresponds to a customer of the computing resource provider; and

the cryptography service is further configured to:

obtain, from customers of the computing resource provider, policy updates; and

update the stored policy information according to the obtained policy updates.

13. A non-transitory computer-readable storage medium comprising instructions that, when executed by one or more processors of a computer system, cause the computer system to at least:

process a policy related to operation of a cryptography service, the policy defining one or more limitations on cryptographic operations performed by the cryptography service;

obtain a request to utilize a service separate from the cryptography service;

cause the cryptography service to use a key to perform, subject to the one or more limitations, one or more cryptographic operations on information that, after the one or more cryptographic operations have been performed, is usable to fulfill the request, the key being inaccessible to the service, the one or more cryptographic operations including providing an identifier of the key to enable the cryptography service to select the key from a plurality of keys stored by the cryptography service, the identifier being provided based at least in part on the one or more limitations; and

fulfill the request to utilize the service using the information.

14. The non-transitory computer-readable storage medium of claim 13, wherein the request includes an attestation that enables the cryptography service to verify, against the policy, that the request to utilize the service is authentic.

15. The non-transitory computer-readable storage medium of claim 13, wherein:

the request to utilize the service includes a request to perform an operation in connection with a data object; and

the information is a key used to encrypt the data object.

16. The non-transitory computer-readable storage medium of claim 13, wherein the instructions, when executed by the one or more processors, further cause the computer system to enforce a plurality of policies that includes the policy.

17. The non-transitory computer-readable storage medium of claim 13, wherein the request to utilize the service is a request to perform a storage operation in connection with a data object.

18. The non-transitory computer-readable storage medium of claim 13, wherein the instructions, when executed by the one or more processors, further cause the computer system to obtain, from a customer device associated with the computer system, a request to update the policy.

19. The non-transitory computer-readable storage medium of claim 18, wherein the request to update the policy is obtained via an application programming interface provided by the computer system.