CLAIMS

WHAT IS CLAIMED IS:

1. A computer-implemented method for providing cryptographic services under the control of one or more computer systems of a first service configured with executable instructions, the method comprising the steps of:

as a result of a second service receiving a first request to utilize the second service, receiving by the first service a second request to perform one or more cryptographic operations that are necessary for fulfilling the first request;

performing by the first service the requested one or more cryptographic operations, based at least in part on proof information configured to enable performance of the requested one or more cryptographic operations, where the proof information is provided by an authentication service and verifiable using a key shared between the first service and the authentication service; and

providing by the first service one or more results of performing the requested one or more cryptographic operations to the second service, the one or more results necessary for at least one manner of fulfilling the received first request to utilize the second service.

2. The computer-implemented method of claim 1, wherein the one or more cryptographic operations include decryption of a further key needed to fulfill the received request to utilize the second service.

3. The computer-implemented method of claim 1 or 2, wherein:

the method further comprises receiving information verifying that the received first request to utilize the second service is authentic; and

performing the one or more cryptographic operations requires receipt of the information verifying that the received second request to utilize the second service is authentic.

4. The computer-implemented method of any one of claims 1 to 3, wherein the received first request to utilize the second service is a request to obtain data stored by the second service.

5. The computer-implemented method of any one of claims 1 to 3, wherein the received first request to utilize the second service is a request to store data using the second service.

6. The computer-implemented method of any one of claims 1 to 5, further comprising selecting, from a plurality of keys that comprises at least two keys each managed by the cryptography service on behalf of a different entity, at least one key for performing the one or more cryptographic operations.

7. The computer-implemented method of any one of claims 1 to 6, wherein:

the one or more cryptographic operations require use of an encryption key;

the method further comprises receiving, for the encryption key, a policy for the encryption key; and

performing the one or more cryptographic operations requires performance of the one or more cryptographic operations to be in compliance with the received policy.

8. The computer-implemented method of any one of claims 1 to 6, further comprising:

receiving a policy for an encryption key usable to perform the one or more cryptographic operations;

checking whether an existing policy allows implementation of the policy; and

rejecting the received policy as a result of the existing policy disallowing implementation of the policy.

9. A computer system, comprising:

a first service receiving a second request to perform one or more cryptographic operations, the second request being received as a result of a second service receiving a first request to utilize the second service and the one or more cryptographic operations being necessary for fulfilling the first request; and

an authentication service for providing proof information to the first service, wherein the first service is configured to at least:

perform the requested one or more cryptographic operations based at least in part on the proof information, where the proof information is verifiable using a key shared between the first service and the authentication service; and

providing one or more results of performing the requested one or more cryptographic operations to the second service, the one or more results necessary for at least one manner of fulfilling the received request to utilize the second service, wherein the cryptography service is configured to at least:

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

upon detecting a request pending at the first service:

determining whether the proof information is authentic;

as a result of determining that the proof information is authentic, selecting one of the plurality of encryption keys and using the selected encryption key to perform the one or more cryptographic operations needed to fulfill the pending request.

10. The computer system of claim 9, wherein detecting the request pending at the first service includes receiving, from the first service, notification and proof of the request pending at the first service.

11. The computer system of any one of claims 9 and 10, wherein the cryptography service is further configured to verify that the pending request is authorized.

12. The computer system of any one of claims 9 to 11, further comprising a metering service configured to receive output of the cryptography service and generate accounting records based at least in part on the received output.

13. The computer system of any one of claims 9 to 12, wherein the cryptography service is further configured to:

store policy information that defines one or more policies for each of at least a subset of the plurality of encryption keys; and

enforce the defined one or more policies.

14. The computer system of claim 13, wherein:

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

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

the cryptography service is configured to:

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

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