

CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:
 - 5 a first data storage service comprising a plurality of data storage devices
and a first web service interface configured to receive web service requests
transmitted to the first web service interface, the first data storage service
being configured to process the web service requests transmitted to the first
web service interface using the plurality of data storage devices; and
 - 10 a second data storage service, where first data storage service is
implemented with computing resources in a first set of one or more facilities
operated by a computing resource service provider and the second data
storage service is implemented with computing resources in a second set of
one or more facilities that is geographically distinct from the first set of one or
15 more facilities and operated by the computing resource service provider and
the first data storage service is configured in accordance with a first set of
regulations associated with a first legal jurisdiction and the second data storage
service is configured in accordance with a second set of regulations that is
different from the first set of regulations and associated with a second legal
20 jurisdiction, the second data storage service comprising a second web service

interface, the second data storage service configured to operate as a proxy to the first data storage service by at least:

- receiving, at the second web service interface, a request from a requestor to store data, the request originating from a network not operated by the service provider;
- encrypting the data using a cryptographic key inaccessible to the first data storage service;
- transmitting the encrypted data to the first data storage service for persistent storage on behalf of the requestor; and
- maintaining access to the cryptographic key while preventing access to the cryptographic key by the first data storage service.

2. The system of claim 1, wherein both the first web service interface and the second web service interface are each publicly addressable interfaces in a public communications network.

3. The system of claim 1, wherein the second data storage service is configured to encrypt the data without requiring the requestor to specify that the data should be encrypted.

4. The system of claim 1, wherein the second data storage service is further configured to:
- receive, to the second web service interface, a request to retrieve the data;
- 5 obtain the encrypted data from the first data storage service;
- use the key to decrypt the encrypted data; and
- provide the decrypted data.
5. The system of claim 1, wherein the first data storage service and second data
- 10 storage service are implemented in different legal jurisdictions.
6. A system, comprising:
- one or more processors; and
- memory comprising computer executable instructions that, when
- 15 executed by the one or more processors, cause the system to:
- operate, by a service provider, an application programming interface to which requests are submittable over a network, the request originating from a network not operated by the service provider; and
- for each first request of at least a plurality of requests submitted
- 20 to the application programming interface, process the first request by at least:

using a key to perform one or more cryptographic
operations on data involved in processing the first request; and
transmitting, across a network, a second request to a
service utilizing separate computing resources than the
5 application programming interface that causes the service to
perform one or more operations on the data in encrypted form
wherein the separate computing resources are located in a first
location governed by different regulations than a second
location where the application programming interface is located,
10 the service lacking access to the key and being configured to be
independently configured to process the first request.

7. The system of claim 6, wherein:

the system is operated as part of a first instance of a service type
15 provided by the service provider; and

the service is operated as part of a second instance of the service type
provided by the service provider.

8. The system of claim 6, wherein the application programming interface is a web
20 service interface.

9. The system of claim 6, wherein:

at least some of the plurality of requests are transmitted by different entities; and

each different entity corresponds to an account of the service.

5

10. The system of claim 6, wherein:

the executable instructions further cause the system to selectively determine whether to perform the one or more cryptographic operations when processing requests; and

10

the plurality of requests are a subset of a set of requests processed by the system, the subset consisting of requests for which the system has selectively determined to perform the one or more cryptographic operations.

11. The system of claim 6, wherein the executable instructions further cause the

15

system to select the service from a plurality of services configured to process the first request.

12. The system of claim 6, wherein:

the second request to the service causes the service to perform one or

20

more operations on unencrypted data and provide, to the system, a result of performing the one or more operations and the data in encrypted form;

wherein using the key to perform the one or more cryptographic operations includes decrypting the data in encrypted form; and

the executable instructions further cause the system to perform one or more operations on a collection of data comprising the unencrypted data and the decrypted data.

13. The system of claim 6, wherein the service is operated by a first organizational entity that is different from the service provider that operates the system.

14. The system of claim 6, wherein the memory further includes instructions that, when executed by the one or more processors cause the system to analyze the request to determine whether to restrict access by the first data storage service to a subset of the data in encrypted form.

15. A computer-implemented method, comprising:

under the control of one or more computer systems configured with executable instructions,

receiving, from a requestor at a network address of the one or more computer systems, an application programming interface request to perform one or more operations, where the network address originates from a network that is not operated by a service provider

wherein the network is located in a first location governed by different regulations than a second location where the application programming interface is located; and

processing the application programming interface request by at

5 least:

transmitting, over the network, a request to a service operated by the service provider that is configured to be independently configured to perform the one or more operations, the request being configured to causes the service to perform one or more service operations on encrypted data, the encrypted data being encrypted under a key that is inaccessible to the service; and

10

using the key to perform one or more cryptographic operations in connection with the encrypted data.

15

16. The computer-implemented method of claim 15, wherein:

the one or more cryptographic operations include encryption of data to obtain the encrypted data; and

the one or more service operations include persistent storage of the encrypted data.

20

17. The computer-implemented method of claim 15, wherein the network address is a public Internet protocol address.
18. The computer-implemented method of claim 15, wherein the method further
5 comprises selecting the service from a plurality of services each independently configured to perform the one or more operations.
19. The computer-implemented method of claim 15, wherein performing the one or more cryptographic operations includes transmitting, over the network to a
10 cryptography service, a request that causes the cryptography service to perform one or more other cryptographic operations using cryptographic information that is inaccessible to both the one or more computer systems and the service.
- 15 20. The computer-implemented method of claim 15, wherein the network address is associated with a string that is usable for obtaining the network address from a domain name service, the string being unassociated with a network address for the service by any domain name service.
- 20 21. One or more non-transitory computer-readable storage media having collectively stored therein computer executable instructions that, when

executed by one or more processors of a computer system, cause the computer system to:

provide an application programming interface accessible at a network address;

5 receive, at the application programming interface, an application programming interface request, from a requestor, to perform one or more operations on a set of data, the application programming interface request originating from a network that is not associated with the network address and governed by different regulations; and

10 fulfill the received application programming interface request, at least in part by:

causing at least a subset of the set of data to be encrypted under a key kept inaccessible to a remote service; and

utilizing the remote service operated by a service provider
15 distinct from the requestor to perform at least a subset of the one or more operations on the set of data such that, for the subset of the set of data, the remote service has access to the subset of the set of data only in encrypted form.

20 22. The one or more non-transitory computer-readable storage media of claim 21, wherein:

the network address is a public Internet protocol address; and
utilizing the remote service includes transmitting a request to the
remote service addressed to a public Internet protocol address of the remote
service.

5

23. The one or more non-transitory computer-readable storage media of claim 21,
wherein the remote service is independently configured to perform a
requested operation as indicated in the application programming interface
request for the requestor.

10

24. The one or more non-transitory computer-readable storage media of claim 21,
wherein:

the computer executable instructions further cause the computer
system to analyze the application programming interface request to determine
whether to restrict access by the remote service to the subset of the data in
encrypted form; and

15

the remote service only having access to the subset of the data in
encrypted form as a result of determining to restrict access by the remote
service to the subset of the data in encrypted form.

20

25. The one or more non-transitory computer-readable storage media of claim 24,
wherein:

as a result of determining to restrict access by the remote service to the
subset, the instructions further cause the computer system to determine,
5 based at least in part on analysis of the application programming interface
request, an encryption key; and
restricting access by the remote service includes encrypting at least a
portion of the subset using the determined encryption key.

10 26. The one or more non-transitory computer-readable storage media of claim 21,
wherein:

a plurality of services that include the remote service are configured to
be utilized by the computer system for fulfilling the application programming
interface request; and

15 the computer executable instructions further cause the computer
system to select, from the plurality of services, the remote service based at
least in part on a configuration setting specific to the requestor.

27. The one or more non-transitory computer-readable storage media of claim 21,
20 wherein:

the computer executable instructions further cause the computer system to encrypt the subset of the set of data using the key; and

utilizing the remote service to perform one or more operations includes submitting a storage request to the remote service to store the set of data.