WHAT IS CLAIMED IS:

1. A system, comprising one or more computing devices of a provider network operable to implement a network-accessible service for generating random data, wherein the one or more computing devices are configured to:

implement one or more programmatic interfaces enabling a determination of respective characteristics of random data to be provided to one or more clients of the service;

implement one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtain, on behalf of the particular client, random data from one or more servers of the provider network designated as random data producers for the one or more clients; and

initiate a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client, in accordance with a security protocol determined for the transmission.

2. The system as recited in claim 1, wherein the one or more programmatic interfaces include a particular programmatic interface enabling the particular client to indicate a desired statistical property of the random data to be provided to the particular client.

3. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine, based at least in part on an interaction via a particular programmatic interface of the one or more programmatic interfaces, a type of application for which the random data is to be employed on behalf of the particular client; and

determine, based on the type of application, one or more characteristics of the random data to be provided to the particular client.

4. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine one or more entropy sources to be used by at least one server of the one or more servers to generate the random data on behalf of the particular client.

5. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine the security protocol to be used for the transmission of the random data in accordance with target levels of confidentiality, authenticity, data integrity and replay protection based at least in part on one or more of: (a) security preferences indicated by the particular client, (b) inferred security requirement characteristics associated with the particular client, or (c) a network address associated with the destination.

6. A method, comprising:

implementing one or more programmatic interfaces enabling a determination of respective characteristics of random data to be delivered to one or more clients of a random data service of a provider network;

implementing one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and,

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtaining, on behalf of the particular client, random data from one or more servers of the provider network; and

initiating a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client.

7. The method as recited in claim 6, further comprising:

determining, based at least in part on an interaction via a particular programmatic interface of the one or more programmatic interfaces, a type of application for which the random data is to be employed on behalf of the particular client; and

determining, based on the type of application, one or more characteristics of the random data to be provided to the particular client.

8. The method as recited in claim 6, further comprising:

designating a set of servers of the provider network, including the one or more servers, as members of a pool of random data producers configured to provide random data for a plurality of clients; and

selecting the one or more servers from the pool in accordance with a producer selection criterion.

9. The method as recited in claim 6, further comprising:

determining a particular security protocol of the one or more security protocols to be used for the transmission of the random data based at least in part on one or more of: (a) security preferences indicated by the particular client, (b) inferred security requirement characteristics associated with the particular client, or (c) a network address associated with the destination, and wherein the particular security protocol is based at least in part on an industry-standard security mechanism providing support for a targeted level of confidentiality, authenticity, data integrity or replay protection.

10. The method as recited in claim 6, further comprising:

implementing a particular programmatic interface for the transmission of the random data to the destination associated with the particular client; and

initiating the transmission of the random data in accordance with the particular programmatic interface.

11. The method as recited in claim 10, wherein the destination comprises an intermediary component at a host at which a client application of the particular client executes, wherein the client application is configured to obtain random data from the intermediary component using a different programmatic interface, further comprising:

submitting, by the intermediary component, a request in accordance with the particular programmatic interface to obtain the random data; and

providing, by the intermediary component to the client application via the different programmatic interface, at least a portion of the random data, without modification of the client application.

12. The method as recited in claim 6, wherein the particular client comprises a software component executing on a particular host, wherein the destination associated with the particular client comprises a local aggregator executing on the particular host, further comprising:

combining, by the local aggregator at the particular host, the random data transmitted by the service, with additional random data generated locally at the particular host; and

providing, to the application by the local aggregator, a result of the combination of the random data transmitted by the service and the random data generated locally.

13. The method as recited in claim 12, wherein the additional random data is generated locally based at least in part on a sequence of data values obtained from a local entropy source, wherein said combining comprises including the random data transmitted by the service in the sequence.

14. The method as recited in claim 6, wherein the one or more servers from which the random data is obtained comprise a plurality of servers, further comprising:

combining, at an aggregator server of the provider network, random data generated at a first server of the plurality of servers with random data generated at a second server of the plurality of servers; and

providing, to the destination from the aggregator server, a result of the combination of the random data transmitted by the first and second servers.

15. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors:

implement one or more programmatic interfaces enabling a determination of respective characteristics of random data to be delivered to one or more clients of a random data service of a provider network;

implement one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and,

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtain, on behalf of the particular client, random data from one or more servers of the provider network; and

initiate a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client.

5

What is claimed is:

1. A system, comprising one or more computing devices of a provider network operable to implement a network-accessible service for generating random data, wherein the one or more computing devices are configured to:

implement one or more programmatic interfaces enabling a determination of respective characteristics of random data to be provided to one or more clients of the service;

implement one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtain, on behalf of the particular client, random data from one or more servers of the provider network designated as random data producers for the one or more clients; and

initiate a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client, in accordance with a security protocol determined for the transmission.

2. The system as recited in claim 1, wherein the one or more programmatic interfaces include a particular programmatic interface enabling the particular client to indicate a desired statistical property of the random data to be provided to the particular client.

3. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine, based at least in part on an interaction via a particular programmatic interface of the one or more programmatic interfaces, a type of application for which the random data is to be employed on behalf of the particular client; and

determine, based on the type of application, one or more characteristics of the random data to be provided to the particular client.

4. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine one or more entropy sources to be used by at least one server of the one or more servers to generate the random data on behalf of the particular client.

5. The system as recited in claim 1, wherein the one or more computing devices are configured to:

determine the security protocol to be used for the transmission of the random data in accordance with target levels of confidentiality, authenticity, data integrity and replay protection based at least in part on one or more of: (a) security preferences indicated by the particular client, (b) inferred security requirement characteristics associated with the particular client, or (c) a network address associated with the destination.

6. A method, comprising:

implementing one or more programmatic interfaces enabling a determination of respective characteristics of random data to be delivered to one or more clients of a random data service of a provider network;

implementing one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and,

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtaining, on behalf of the particular client, random data from one or more servers of the provider network; and

initiating a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client.

7. The method as recited in claim 6, wherein the one or more programmatic interfaces include a particular programmatic interface enabling the particular client to indicate a desired statistical property of the random data to be provided to the particular client.

8. The method as recited in claim 6, further comprising:

determining, based at least in part on an interaction via a particular programmatic interface of the one or more programmatic interfaces, a type of application for which the random data is to be employed on behalf of the particular client; and

determining, based on the type of application, one or more characteristics of the random data to be provided to the particular client.

9. The method as recited in claim 6, further comprising:

determining one or more candidate entropy sources usable by at least one server of the one or more servers to generate the random data on behalf of the particular client.

10. The method as recited in claim 9, further comprising:

selecting, from the one or more candidate entropy sources, a particular entropy source to be used to generate the random data based at least in part on the determined set of characteristics.

11. The method as recited in claim 6, further comprising:

designating a set of servers of the provider network, including the one or more servers, as members of a pool of random data producers configured to provide random data for a plurality of clients; and

selecting the one or more servers from the pool in accordance with a producer selection criterion.

12. The method as recited in claim 6, further comprising:

determining a particular security protocol of the one or more security protocols to be used for the transmission of the random data based at least in part on one or more of: (a) security preferences indicated by the particular client, (b) inferred security requirement characteristics associated with the particular client, or (c) a network address associated with the destination, and wherein the particular security protocol is based at least in part on an industry-standard security mechanism providing support for a targeted level of confidentiality, authenticity, data integrity or replay protection.

13. The method as recited in claim 6, further comprising:

implementing a programmatic interface enabling clients of the service to select a pricing policy for random data from among a plurality of supported pricing policies; and

determining a billing amount for providing the random data to the destination based at least in part on a particular pricing policy selected by the particular client using the programmatic interface.

14. The method as recited in claim 6, further comprising:

implementing a particular programmatic interface for the transmission of the random data to the destination associated with the particular client; and

initiating the transmission of the random data in accordance with the particular programmatic interface.

15. The method as recited in claim 14, wherein the destination comprises an intermediary component at a host at which a client application of the particular client executes, wherein the client application is configured to obtain random data from the intermediary component using a different programmatic interface, further comprising:

submitting, by the intermediary component, a request in accordance with the particular programmatic interface to obtain the random data; and

providing, by the intermediary component to the client application via the different programmatic interface, at least a portion of the random data, without modification of the client application.

16. The method as recited in claim 14, wherein the destination comprises a client application of the particular client, further comprising:

submitting, by the client application, a request in accordance with the particular programmatic interface to obtain the random data.

17. The method as recited in claim 6, further comprising:

implementing a uniqueness policy associated with providing random data to the one or more clients, wherein the uniqueness policy is targeted at preventing prediction of contents of one set of random data provided by the random data service based on contents of any other set of random data provided by the service.

18. The method as recited in claim 6, wherein the particular client comprises a software component executing on a particular host, wherein the destination associated with the particular client comprises a local aggregator executing on the particular host, further comprising:

combining, by the local aggregator at the particular host, the random data transmitted by the service, with additional random data generated locally at the particular host; and

providing, to an application by the local aggregator, a result of the combination of the random data transmitted by the service and the random data generated locally.

19. The method as recited in claim 18, wherein the additional random data is generated locally based at least in part on a sequence of data values obtained from a local entropy source, wherein said combining comprises including the random data transmitted by the service in the sequence.

20. The method as recited in claim 6, wherein the one or more servers from which the random data is obtained comprise a plurality of servers, further comprising:

combining, at an aggregator server of the provider network, random data generated at a first server of the plurality of servers with random data generated at a second server of the plurality of servers; and

providing, to the destination from the aggregator server, a result of the combination of the random data transmitted by the first and second servers.

21. A non-transitory computer-accessible storage medium storing program instructions that when executed on one or more processors:

implement one or more programmatic interfaces enabling a determination of respective characteristics of random data to be delivered to one or more clients of a random data service of a provider network;

implement one or more security protocols for transmission of random data to the one or more clients, the one or more security protocols including at least one security protocol for transmission of random data to trusted clients at one or more devices resident within the provider network; and,

in accordance with a determined set of characteristics of random data to be provided to a particular client of the one or more clients:

obtain, on behalf of the particular client, random data from one or more servers of the provider network; and

initiate a transmission of the random data obtained from the one or more servers, directed to a destination associated with the particular client.

22. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the one or more security protocols include at least one security protocol for transmission of random data to untrusted clients at one or more devices resident outside the provider network.

23. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the one or more programmatic interfaces include a particular programmatic interface enabling the particular client to indicate a desired statistical property of the random data to be provided to the particular client.

24. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

determine, based at least in part on an interaction via a particular programmatic interface of the one or more programmatic interfaces, a type of application for which the random data is to be employed on behalf of the particular client; and

determine, based on the type of application, one or more characteristics of the random data to be provided to the particular client.

25. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

determine one or more candidate entropy sources usable by at least one server of the one or more servers to generate the random data on behalf of the particular client.

26. The non-transitory computer-accessible storage medium as recited in claim 25, wherein the instructions when executed on the one or more processors:

select, from the one or more candidate entropy sources, a particular entropy source to be used to generate the random data based at least in part on the determined set of characteristics.

27. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

designate a set of servers of the provider network, including the one or more servers, as members of a pool of random data producers configured to provide random data for a plurality of clients; and

select the one or more servers from the pool in accordance with a producer selection criterion.

28. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

determine a particular security protocol of the one or more security protocols to be used for the transmission of the random data based at least in part on one or more of: (a) security preferences indicated by the particular client, (b) inferred security requirement characteristics associated with the particular client, or (c) a network address associated with the destination.

29. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

implement a particular programmatic interface enabling clients of the service to select a pricing policy for random data from among a plurality of supported pricing policies; and

determine a billing amount for providing the random data to the destination based at least in part on a particular pricing policy selected by the particular client using the particular programmatic interface.

30. The non-transitory computer-accessible storage medium as recited in claim 29, wherein the plurality of supported pricing policies includes one or more of: (a) a pricing policy according to which the particular client's billing amount is determined based on an amount of random data provided to the destination, (b) a pricing policy according to which the particular client's billing amount is determined based on a rate at which random data is provided to the destination, (c) a pricing policy according to which the particular client's billing amount is determined based on a quality metric associated with at least a portion of the random data provided to the destination, or (d) a pricing policy according to which the particular client's billing amount is determined based on an entropy source used to obtain at least a portion of the random data provided to the destination.

31. The non-transitory computer-accessible storage medium as recited in claim 21, wherein the instructions when executed on the one or more processors:

implement a particular programmatic interface for the transmission of the random data to the destination associated with the particular client; and

initiate the transmission of the random data in accordance with the particular programmatic interface.