Glossary

BlockSphinxPlaintext

The payload structure which is encapsulated by the Sphinx body.

classes of traffic

We distinguish the following classes of traffic:

- SURB Replies (also sometimes referred to as ACKs)
- Forward messages

client

Software run by the User on its local device to participate in the Mixnet. Again let us reiterate that a client is not considered a "node in the network" at the level of analysis where we are discussing the core mixnet protocol in this here document.

directory authority system

Refers to specific PKI schemes used by Mixminion and Tor.

entry mix, entry node

A mix that has some additional features:

- An entry mix is always the first hop in routes where the message originates from a client.
- An entry mix authenticates client’s direct connections via the mixnet’s wire protocol.
- An entry mix queues reply messages and allows clients to retrieve them later.

epoch

A fixed time interval defined in section 4.2 Sphinx Mix and Provider Key Rotation. The epoch is currently set to 20 minutes. A new PKI document containing public key material is published for each epoch and is valid only for that epoch.

family

Identifier of security domains or entities operating one or more mixes in the network. This is used to inform the path selection algorithm.

group

A finite set of elements and a binary operation that satisfy the properties of closure, associativity, invertability, and the presence of an identity element.

group element

An individual element of the group.

group generator

A group element capable of generating any other element of the group, via repeated applications of the generator and the group operation.

header

The packet header consisting of several components, which convey the information necessary to verify packet integrity and correctly process the packet.

KiB

Defined as 1024 8 bit octets.

Katzenpost

A project to design many improved decryption mixnet protocols.

layer

The layer indicates which network topology layer a particular mix resides in.

message

A variable-length sequence of octets sent anonymously through the network. Short messages are sent in a single packet; long messages are fragmented across multiple packets.

mix descriptor

A database record which describes a component mix.

mix

A cryptographic router that is used to compose a mixnet. Mixes use a cryptographic operation on messages being routed which provides bitwise unlinkability with respect to input versus output messages. Katzenpost is a decryption mixnet that uses the Sphinx cryptographic packet format.

mixnet

A mixnet also known as a mix network is a network of mixes that can be used to build various privacy preserving protocols.

MSL

Maximum segment lifetime, currently set to 120 seconds.

nickname

A nickname string that is unique in the consensus document, see Katzenpost Mix Network Specification section 2.2. Network Topology.

node

Clients are NOT considered nodes in the mix network. However note that network protocols are often layered; in our design documents we describe "mixnet hidden services" which can be operated by mixnet clients. Therefore if you are using node in some adherence to methematical termonology one could conceivably designate a client as a node. That having been said, it would not be appropriate to the discussion of our core mixnet protocol to refer to the clients as nodes.

packet

A Sphinx packet, of fixed length for each class of traffic, carrying a message payload and metadata for routing. Packets are routed anonymously through the mixnet and cryptographically transformed at each hop.

payload

The fixed-length portion of a packet containing an encrypted message or part of a message, to be delivered anonymously.

PKI

Public key infrastructure

provider

A service operated by a third party that Clients communicate directly with to communicate with the Mixnet. It is responsible for Client authentication, forwarding outgoing messages to the Mixnet, and storing incoming messages for the Client. The Provider MUST have the ability to perform cryptographic operations on the relayed messages.

SEDA

Staged Event Driven Architecture. 1. A highly parallelizable computation model. 2. A computational pipeline composed of multiple stages connected by queues utilizing active queue management algorithms that can evict items from the queue based on dwell time or other criteria where each stage is a thread pool. 3. The only correct way to efficiently implement a software based router on general purpose computing hardware.

service mix

A service mix is a mix that has some additional features:

- A service mix is always the last hop in routes where the message originates from a client.

- A service mix runs mixnet services which use a Sphinx SURB based protocol.

SURB

Single use reply block. SURBs are used to achieve recipient anonymity, that is to say, SURBs function as a cryptographic delivery token that you can give to another client entity so that they can send you a message without them knowing your identity or location on the network. See `SPHINXSPEC` and `SPHINX`.

user

An agent using the Katzenpost system.

wire protocol

Refers to our PQ Noise based protocol which currently uses TCP but in the near future will optionally use QUIC. This protocol has messages known as wire protocol `commands`, which are used for various mixnet functions such as sending or retrieving a message, dirauth voting etc. For more information, please see our design doc: wire protocol specification [https://github.com/katzenpost/katzenpost/blob/main/docs/specs/wire-protocol.md]