Katzenpost

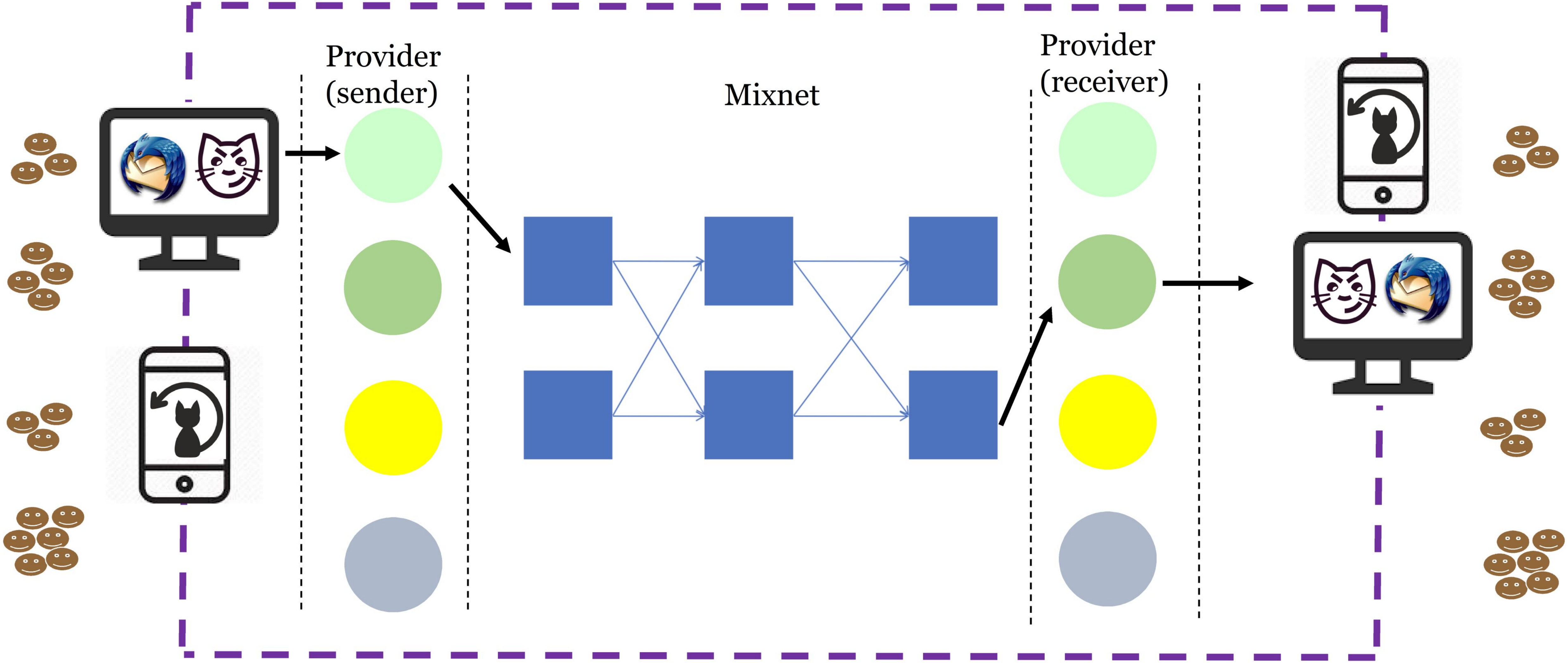
Claudia Diaz

Moritz Bartl

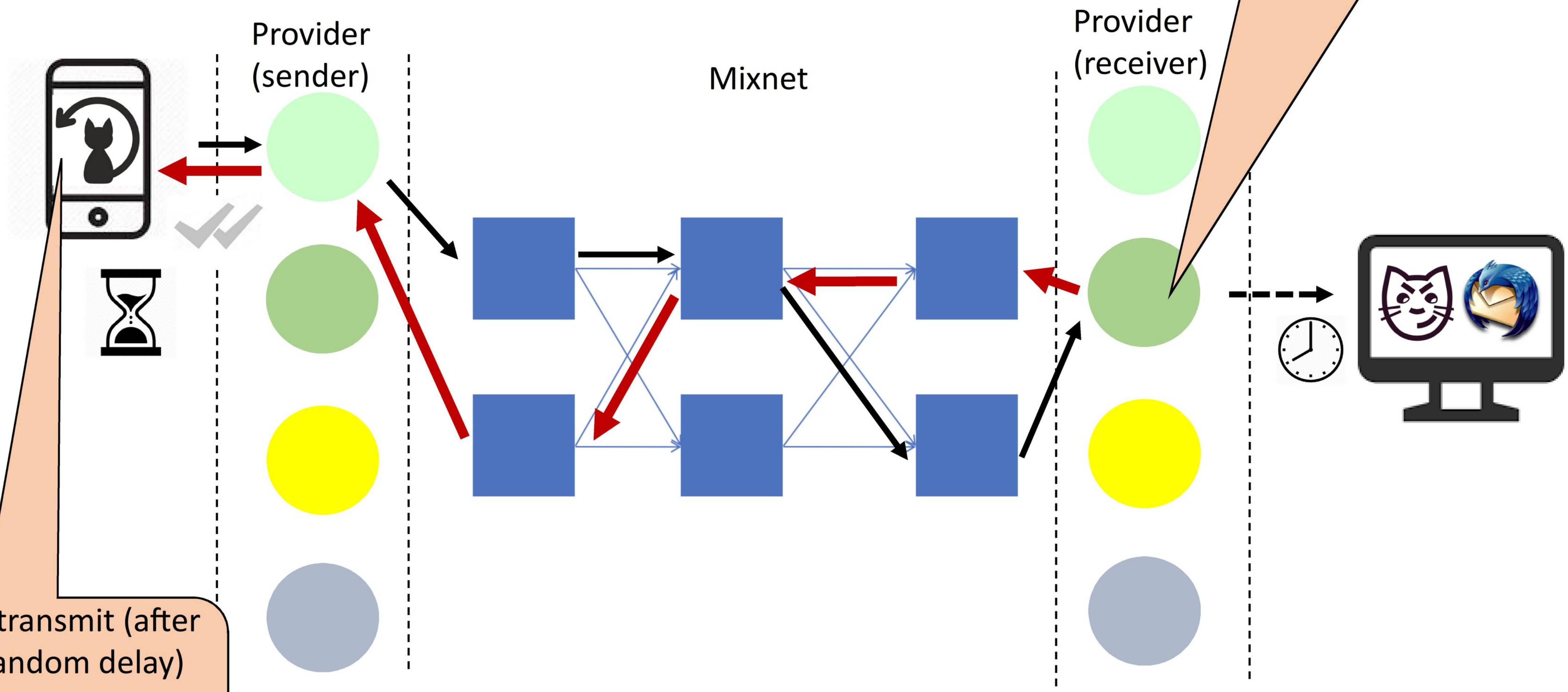
Panoramix meeting

Athens 24 September 2018

Messaging Mixnet Architecture



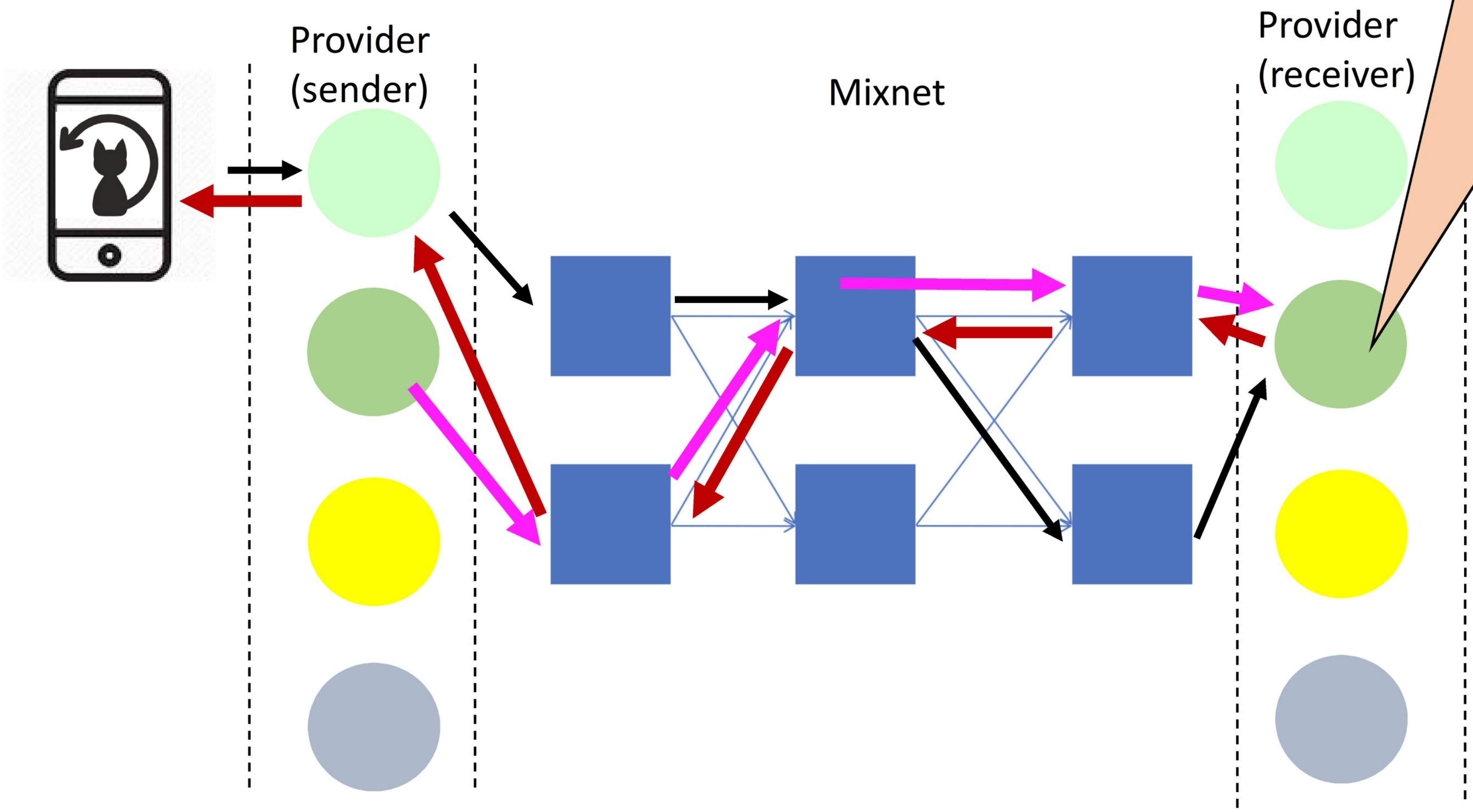
Reliable transport: SURB-AC



Place message to Bob’s inbox
Extract SURB and send back as ACK

Retransmit (after random delay)
Re-encrypt message from scratch

Dummy traffic: loops

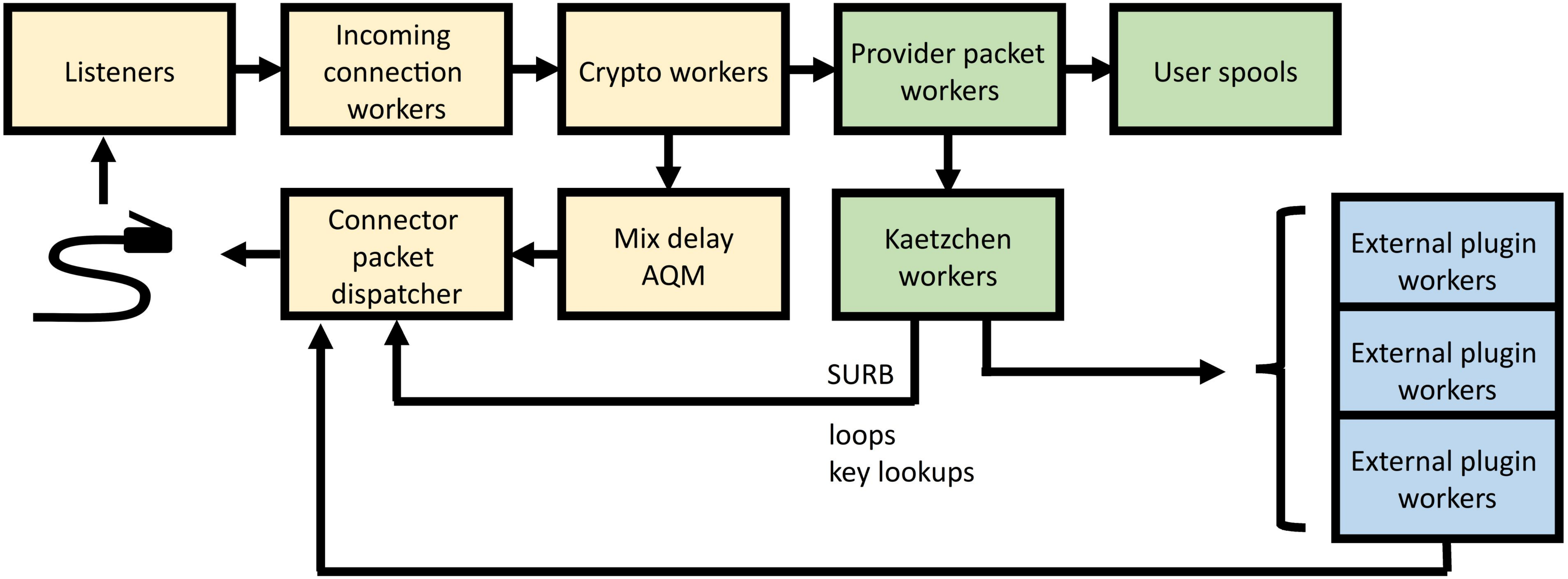


Extract SURB and send back

Messages are indistinguishable from normal user messages for all entities but responding provider

Client loops
Mix loops

Mix and provider pipelines



PKI mixnet infrastructure

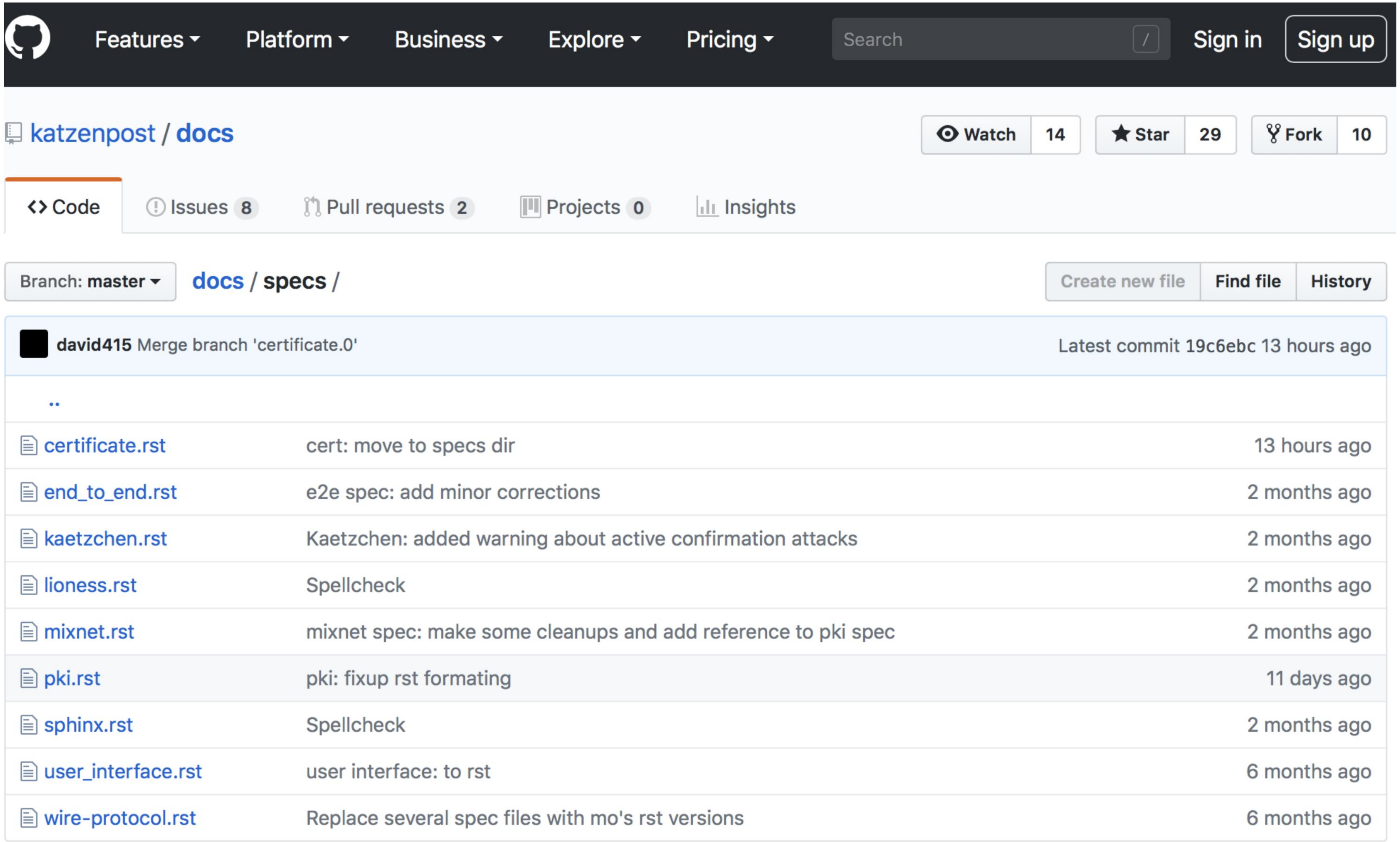
- Directory authorities maintain a consensus on the network
- Consensus lists participating mixes, their descriptors (addresses, crypto keys) and position in the topology
- Published periodically including keys for at least the following 3 epochs
  - nr epochs: max round trip, exposure of keys to compromise attacks
- All key rotations happen simultaneously
- Sphinx key rotation every epoch for forward secrecy and efficient replay protection (mixes & providers)
- Network topology
  - Randomly assigned (based on unbiased random seed)
  - Only refreshed when layers become too unbalanced (splits anonymity sets)
- Mix operators may schedule downtime with half empty mix descriptors

- Open issues:
  - Not byzantine-fault-tolerant, allows for manual intervention upon consensus fault
  - PQ crypto signatures for all PKI documents
  - Packet loss for full current epoch if mix goes down (consensus not updated), worse if long epochs
  - No bandwidth authority to measure actual mix bandwith

PKI Clients

- Providers keep the keys (long lived X25519 keypair) of their users associated to their email address
- Any client can query the key associated to a user account
  - Anonymous lookup over mixnet
  - Indistinguishable from normal message (except for responding provider)
  - Reply uses SURB (similarly to message acks)
- Trust on first use
  - Provider could MITM if it provides bad key
  - Detection possible via self-lookups (probabilistic catching of cheating)

Specs



katzenpost / docs

docs / specs /

david415 Merge branch 'certificate.0' Latest commit 19c6ebc 13 hours ago

..

certificate.rst	cert: move to specs dir	13 hours ago
end_to_end.rst	e2e spec: add minor corrections	2 months ago
kaetzchen.rst	Kaetzchen: added warning about active confirmation attacks	2 months ago
lioness.rst	Spellcheck	2 months ago
mixnet.rst	mixnet spec: make some cleanups and add reference to pki spec	2 months ago
pki.rst	pki: fixup rst formating	11 days ago
sphinx.rst	Spellcheck	2 months ago
user_interface.rst	user interface: to rst	6 months ago
wire-protocol.rst	Replace several spec files with mo's rst versions	6 months ago

Katzenpost Mix Network Wire protocol

- **Fork** of Noise crypto library implementation which has the ability to use the New Hope Simple post quantum hybrid key exchange for forward secrecy
  - addition of a quantum resistant algorithm will provide forward secrecy even in the event that large scale quantum computers are applied to historical intercepts
- Provides
  - Mutual authentication
  - Link layer encryption and forward secrecy
- Used at link layer for ALL communications
  - Clients to Providers and Directory Authorities
  - Providers, Mixes and Directory Authorities

Sphinx

- Compact and secure packet format
- Features:
  - per hop bitwise unlinkability
  - Single Use Reply Blocks
  - indistinguishable replies
  - hidden the path length
  - hidden the relay position
  - tagging attack detection
  - replay attack detection

Mixnet spec

- Network topology (layered)
- Mixing strategy (Poisson)
- Sphinx packet processing
  - Timestamping
  - Authenticate and decrypt
  - Replay detection
  - Keep for specified delay, then forward to next hop
- Scalability
  - Active queue management algorithms (AQMs) in ingress mix and egress queues
  - Messages are purged from (any of) the queues so that performance degrades gracefully with respect to increased work load

E2E spec

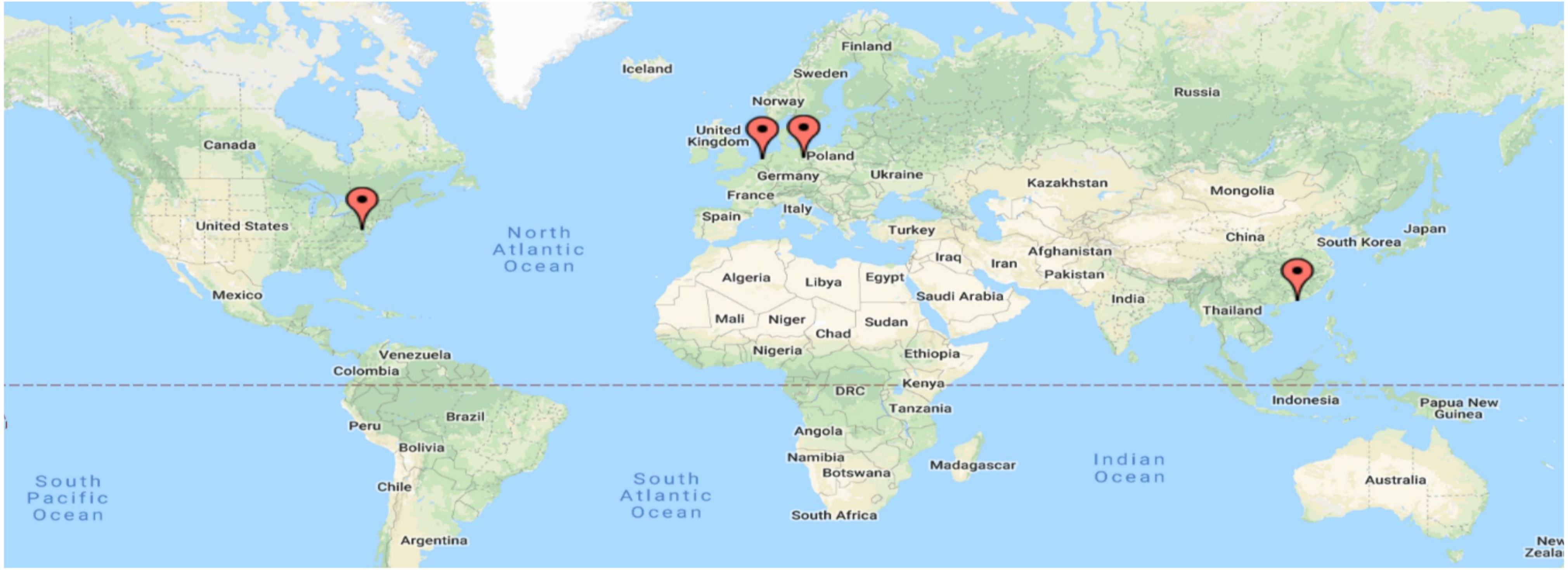
- Sending a message
  - Fragment message into fixed sized blocks
  - Encrypt and authenticate each block
  - Choose route and delays at each hop
    - Open issue: delays for multi-block messages
  - Create the SURB-ACK
  - Assemble ciphertext and SURB-ACK in Sphinx packet payload
  - … Retransmit if needed (ACK not received)
- Receiving a message
  - Provider unwraps sphinx packet and extracts
    - Message block (to receiver mailbox)
    - SURB-ACK (send back to network)
  - Clients poll their provider to download received messages and acks of sent messages
    - Decrypt blocks with user key
    - Reassemble multi-block messages

Downloads

- “Playground” Client Release https://katzenpost.mixnetworks.org/downloads.html
  - Linux / Mac (/ Windows ?) binaries
  - Android integration demo based on K-9 Mail

Playground

- Provided by CCT & Greenhost



Registration

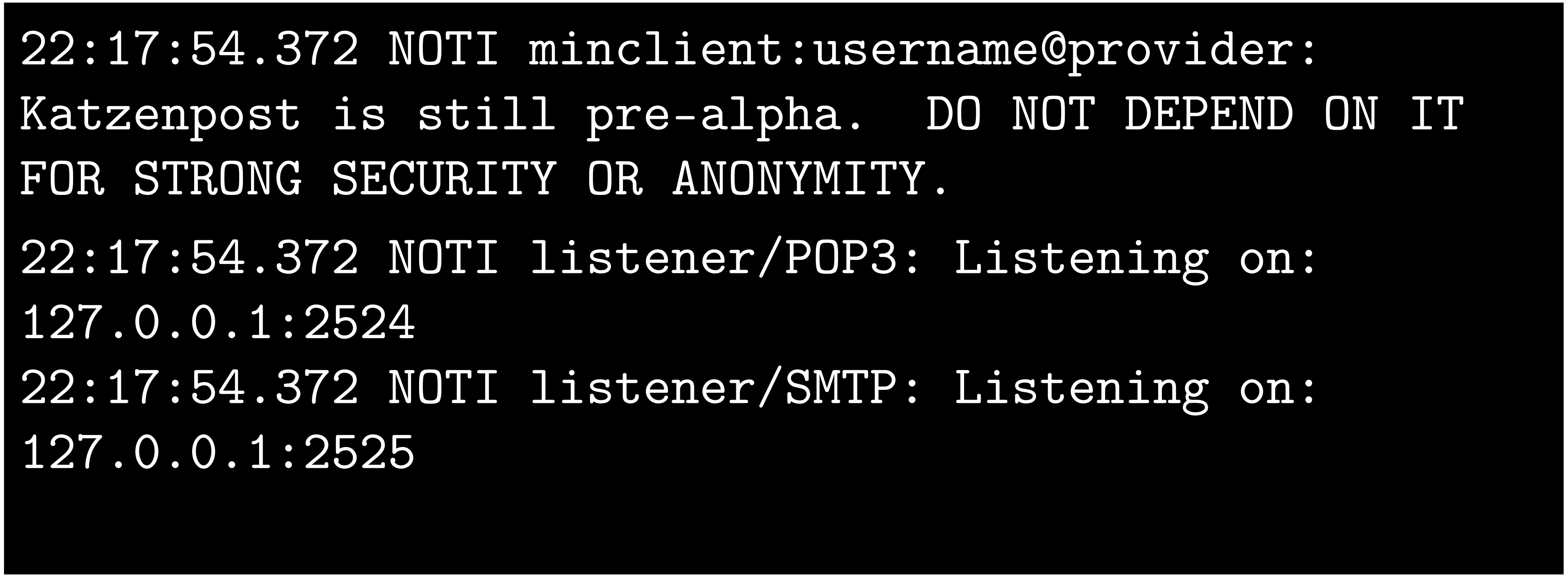
- username@provider

- uploads key to provider
  - authentication
  - keyserver lookups
- writes local configuration file for mailproxy

```
katzenpost_registration -name username
```

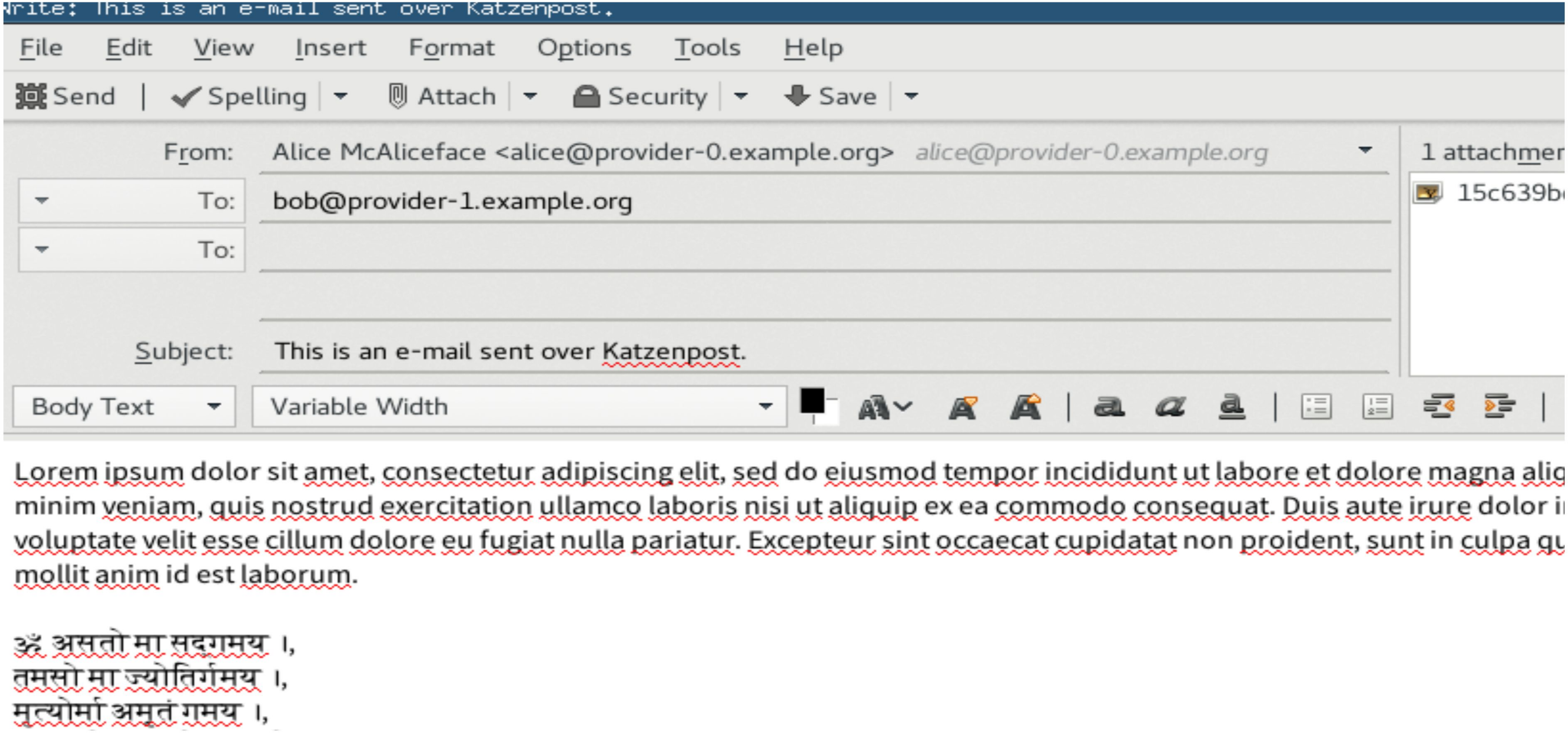
Usage

- `mailproxy -f ~/.mailproxy/mailproxy.toml`



```
22:17:54.372 NOTI minclient:username@provider:
Katzenpost is still pre-alpha.  DO NOT DEPEND ON IT
FOR STRONG SECURITY OR ANONYMITY.
22:17:54.372 NOTI listener/POP3: Listening on:
127.0.0.1:2524
22:17:54.372 NOTI listener/SMTP: Listening on:
127.0.0.1:2525
```

Thunderbird Demo



Write: This is an e-mail sent over Katzenpost.

From: Alice McAliceface <alice@provider-0.example.org> alice@provider-0.example.org

To: bob@provider-1.example.org

To:

Subject: This is an e-mail sent over Katzenpost.

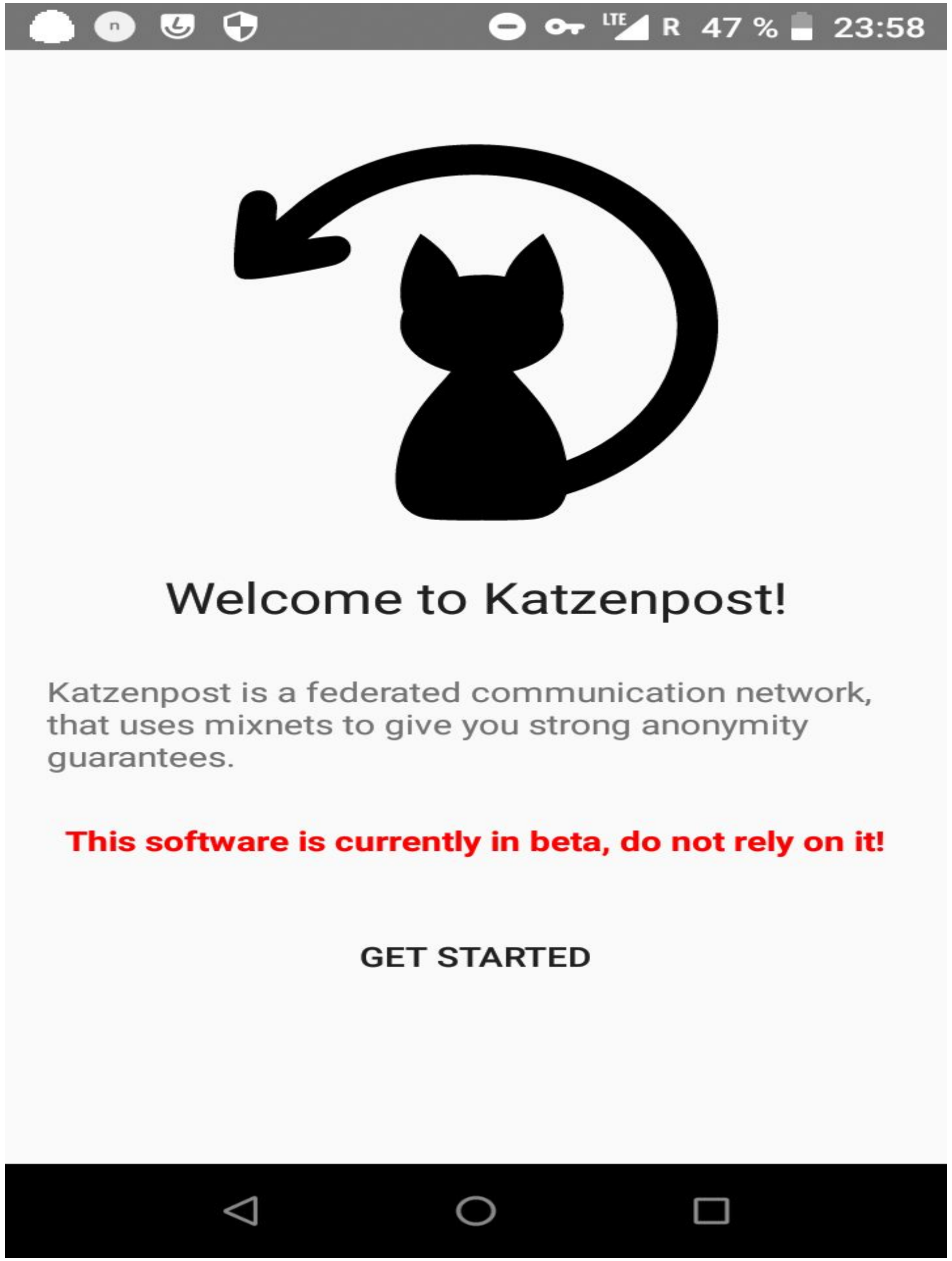
1 attachmer

15c639b

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliq
minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor i
voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qu
mollit anim id est laborum.

ॐ असतो मा सदगमय ।,
तमसो मा ज्योतिर्गमय ।,
मृत्योर्मा अमृतं गमय ।,

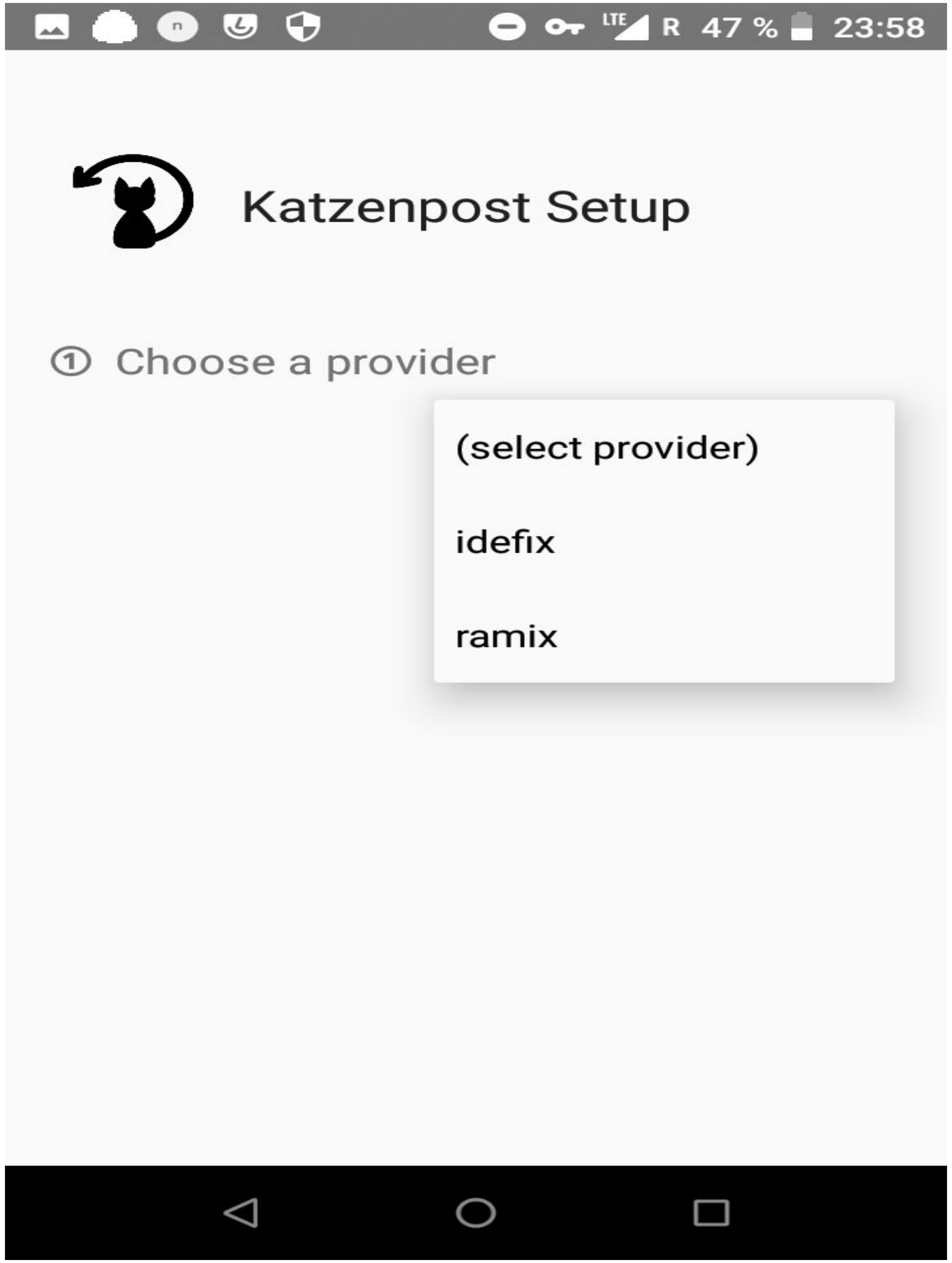
Android



Welcome to Katzenpost!

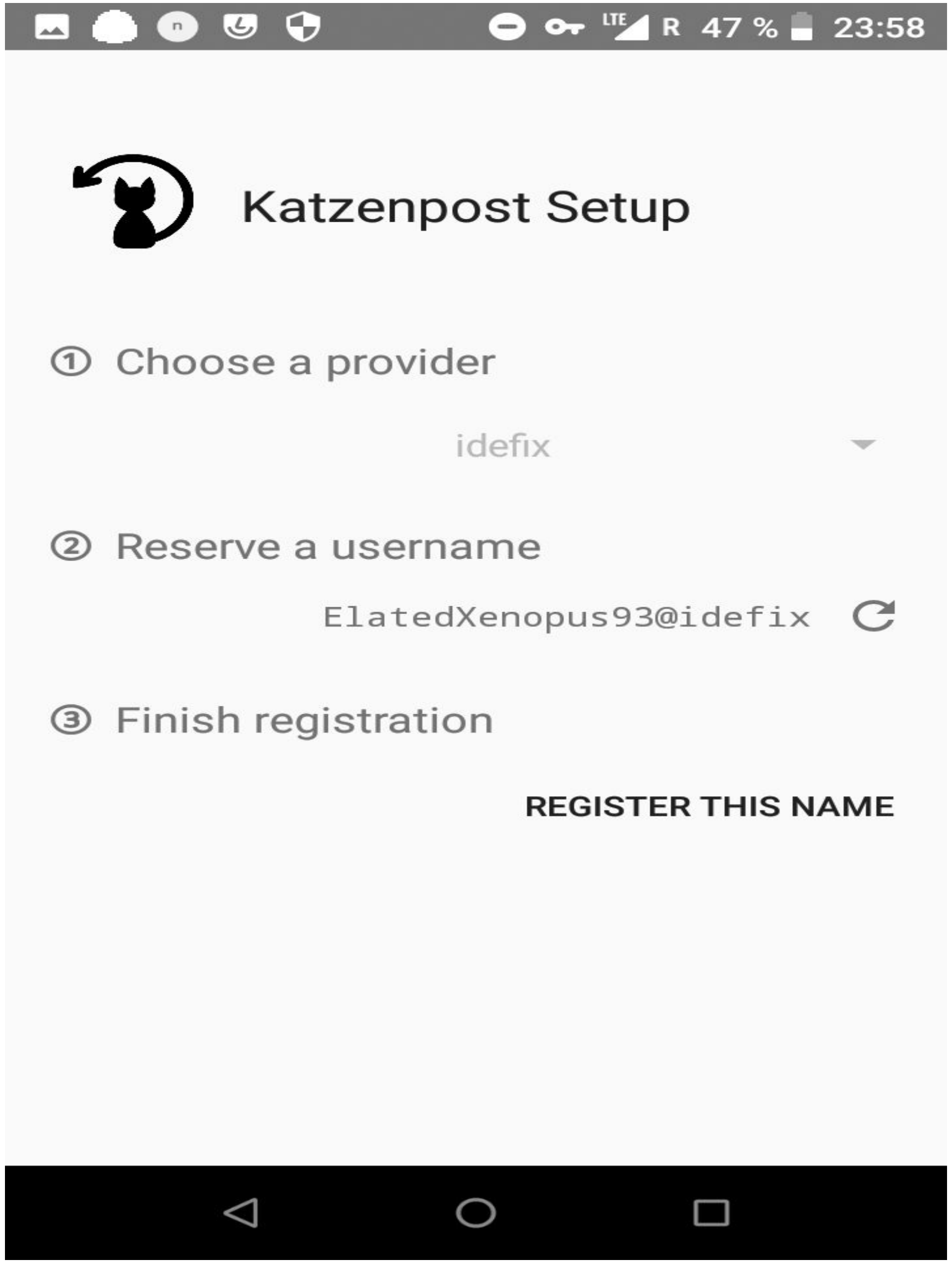
Katzenpost is a federated communication network, that uses mixnets to give you strong anonymity guarantees.

This software is currently in beta, do not rely on it!



Katzenpost Setup

① Choose a provider



Katzenpost Setup

① Choose a provider

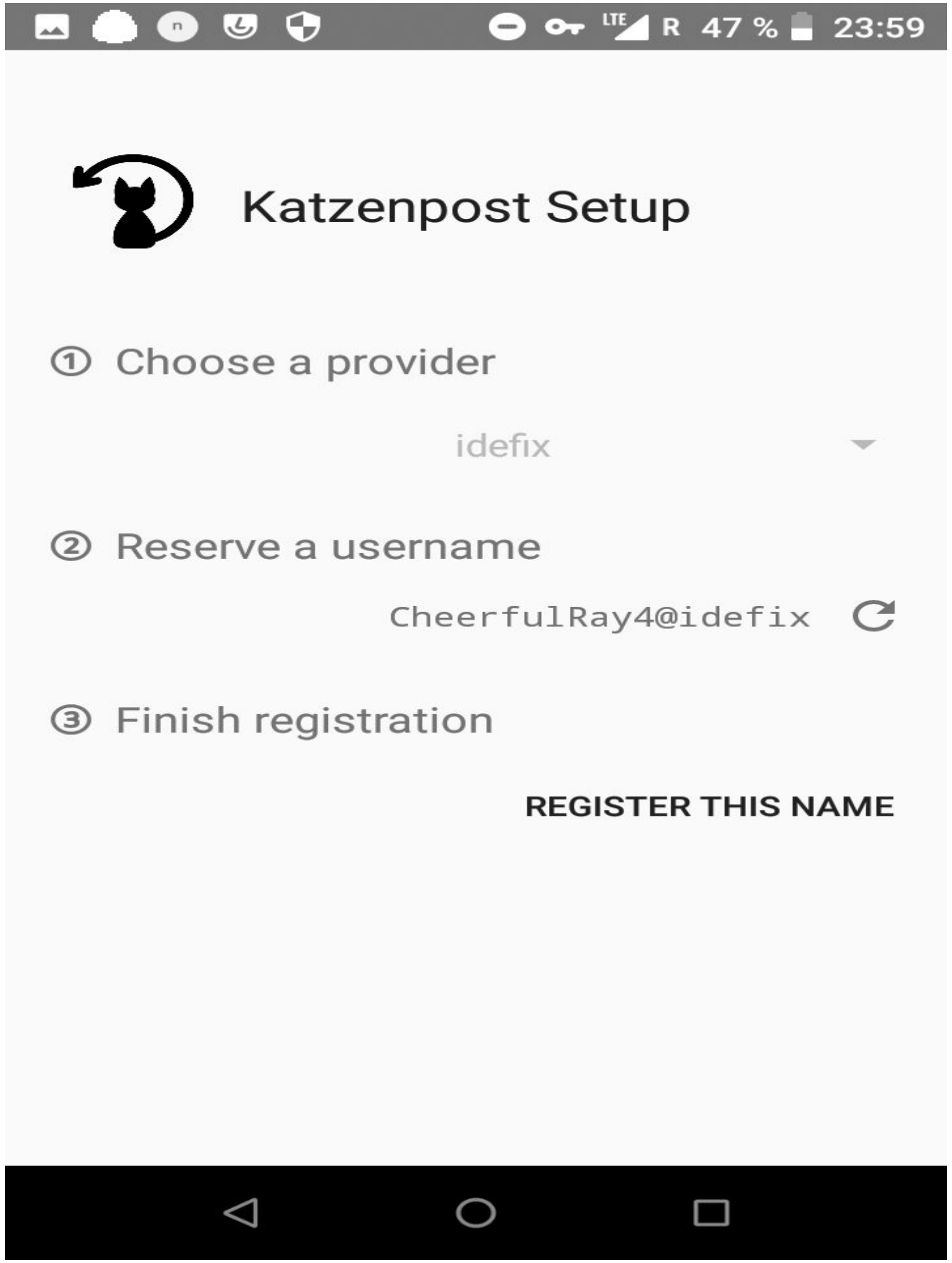
idefix

② Reserve a username

ElatedXenopus93@idefix

③ Finish registration

REGISTER THIS NAME



Katzenpost Setup

① Choose a provider

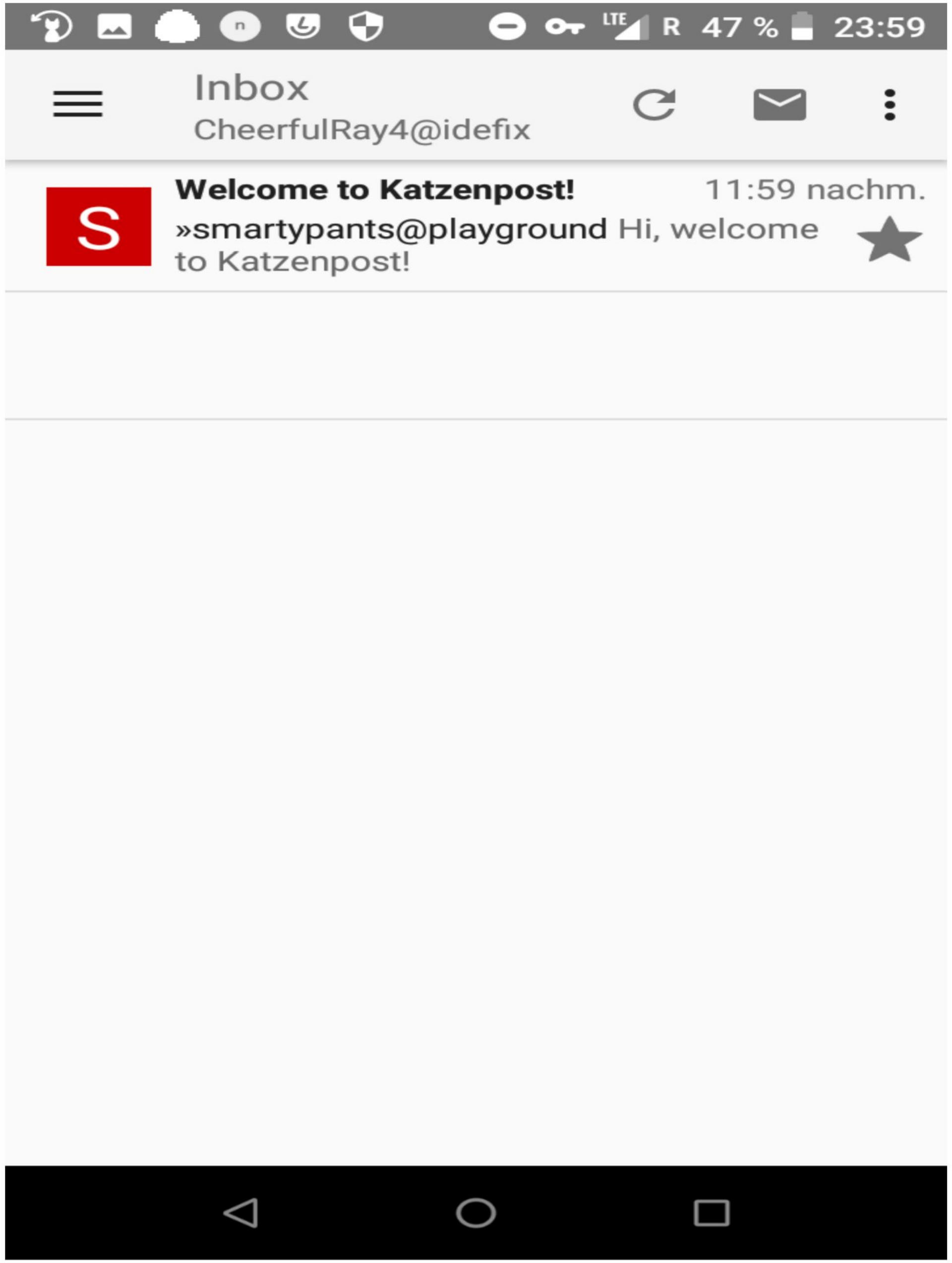
idefix

② Reserve a username

CheerfulRay4@idefix

③ Finish registration

REGISTER THIS NAME



Inbox
CheerfulRay4@idefix

Welcome to Katzenpost! 11:59 nachm.
»smartypants@playground Hi, welcome to Katzenpost!

Documentation

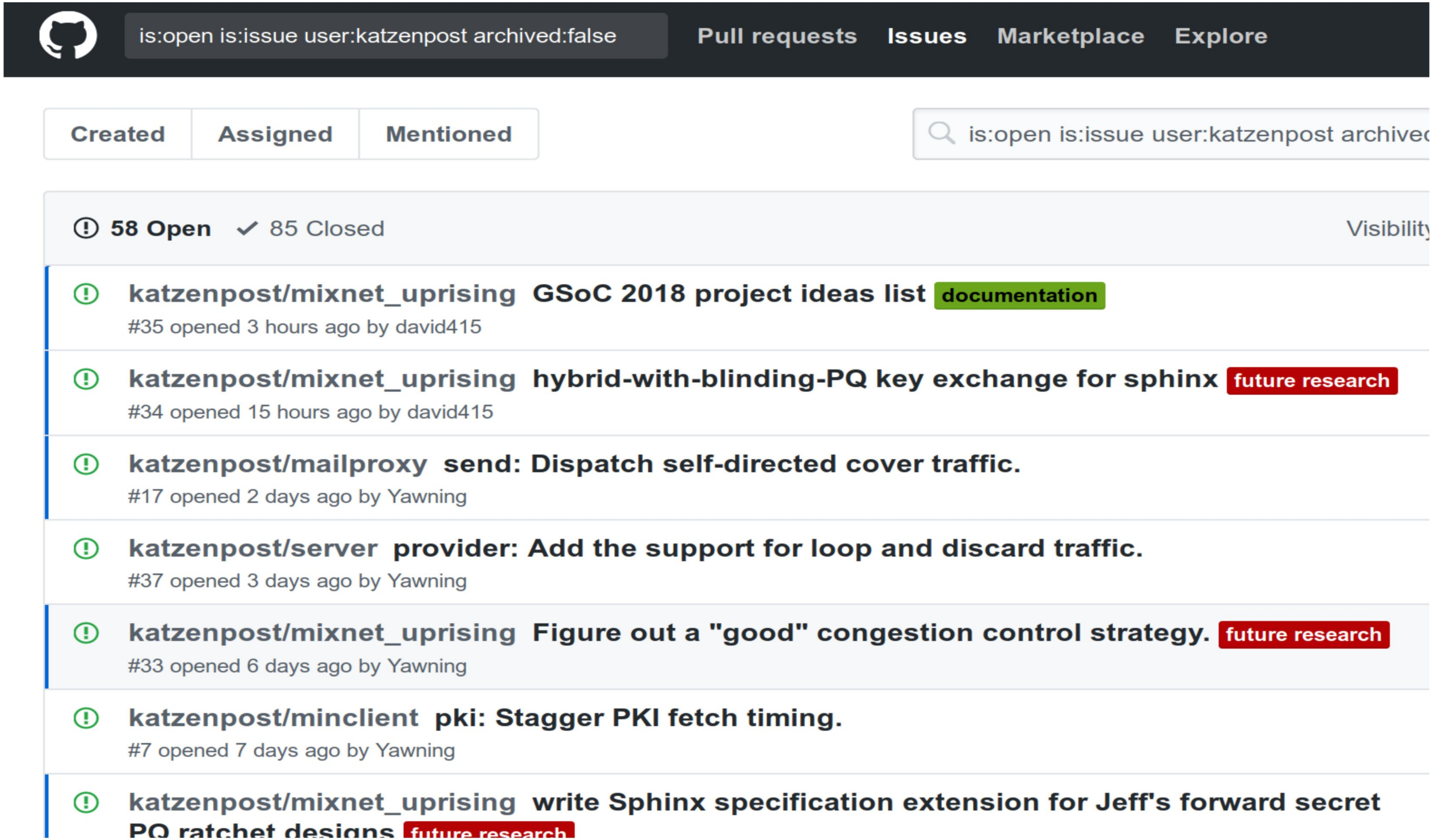
- “Katzenpost Handbook”
- “Getting started in Katzenpost development”
- “How to set up your own Katzenpost mixnet”
- FAQ
- Glossary
- Contribution Guidelines

Specifications

- End-to-end protocol
- Mix network
- Public Key Infrastructure (voting/non-voting)
- Sphinx packet format/SURBs
- Mailproxy (“User Interface”)
- Wire Protocol
- LIONESS Wide-Block-Cipher
- Extensions (Autoresponder/Bot/Echo)

“Proper” Free Software Project

- Active Issue tracker (Github)
- Continuous Integration (TravisCI)
- Mailing lists, Discussion Channel (IRC)



is:open is:issue user:katzenpost archived:false

is:open is:issue user:katzenpost archived

58 Open ✓ 85 Closed

katzenpost/mixnet_uprising GSoC 2018 project ideas list documentation
#35 opened 3 hours ago by david415

katzenpost/mixnet_uprising hybrid-with-blinding-PQ key exchange for sphinx future research
#34 opened 15 hours ago by david415

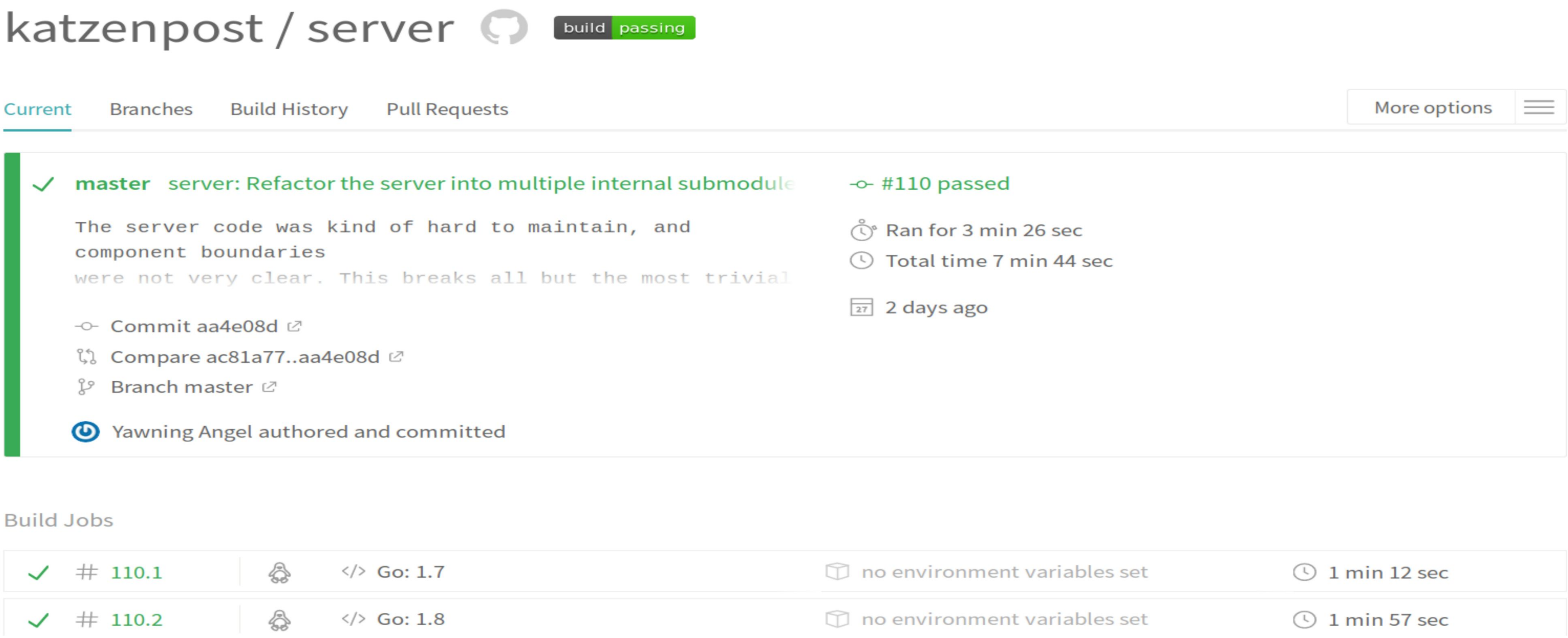
katzenpost/mailproxy send: Dispatch self-directed cover traffic.
#17 opened 2 days ago by Yawning

katzenpost/server provider: Add the support for loop and discard traffic.
#37 opened 3 days ago by Yawning

katzenpost/mixnet_uprising Figure out a "good" congestion control strategy. future research
#33 opened 6 days ago by Yawning

katzenpost/minclient pki: Stagger PKI fetch timing.
#7 opened 7 days ago by Yawning

katzenpost/mixnet_uprising write Sphinx specification extension for Jeff's forward secret PQ ratchet designs future research



katzenpost / server

✓ master server: Refactor the server into multiple internal submodule

The server code was kind of hard to maintain, and component boundaries
were not very clear. This breaks all but the most trivial

Commit aa4e08d

Compare ac81a77..aa4e08d

Branch master

Yawning Angel authored and committed

#110 passed

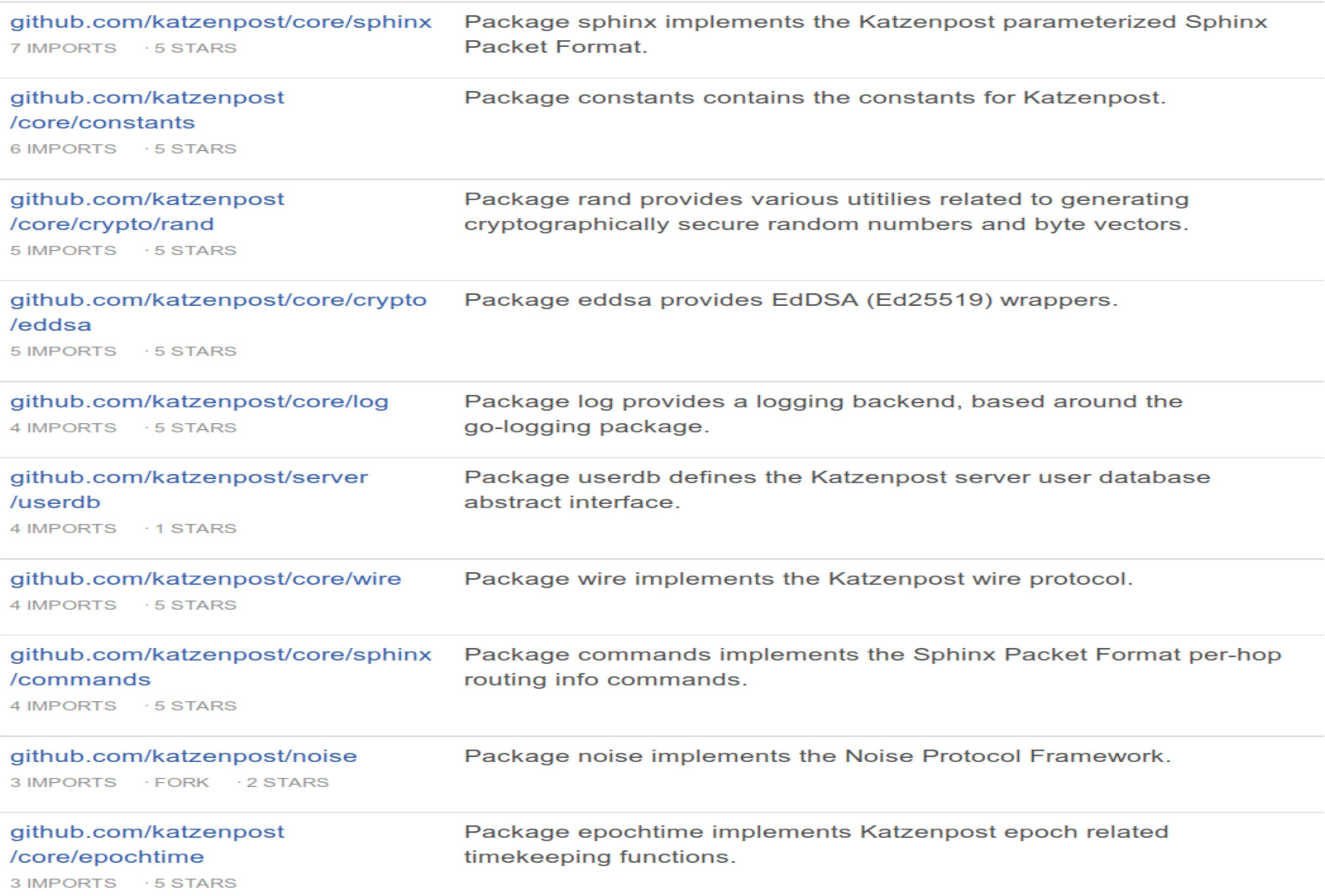
Ran for 3 min 26 sec

Total time 7 min 44 sec

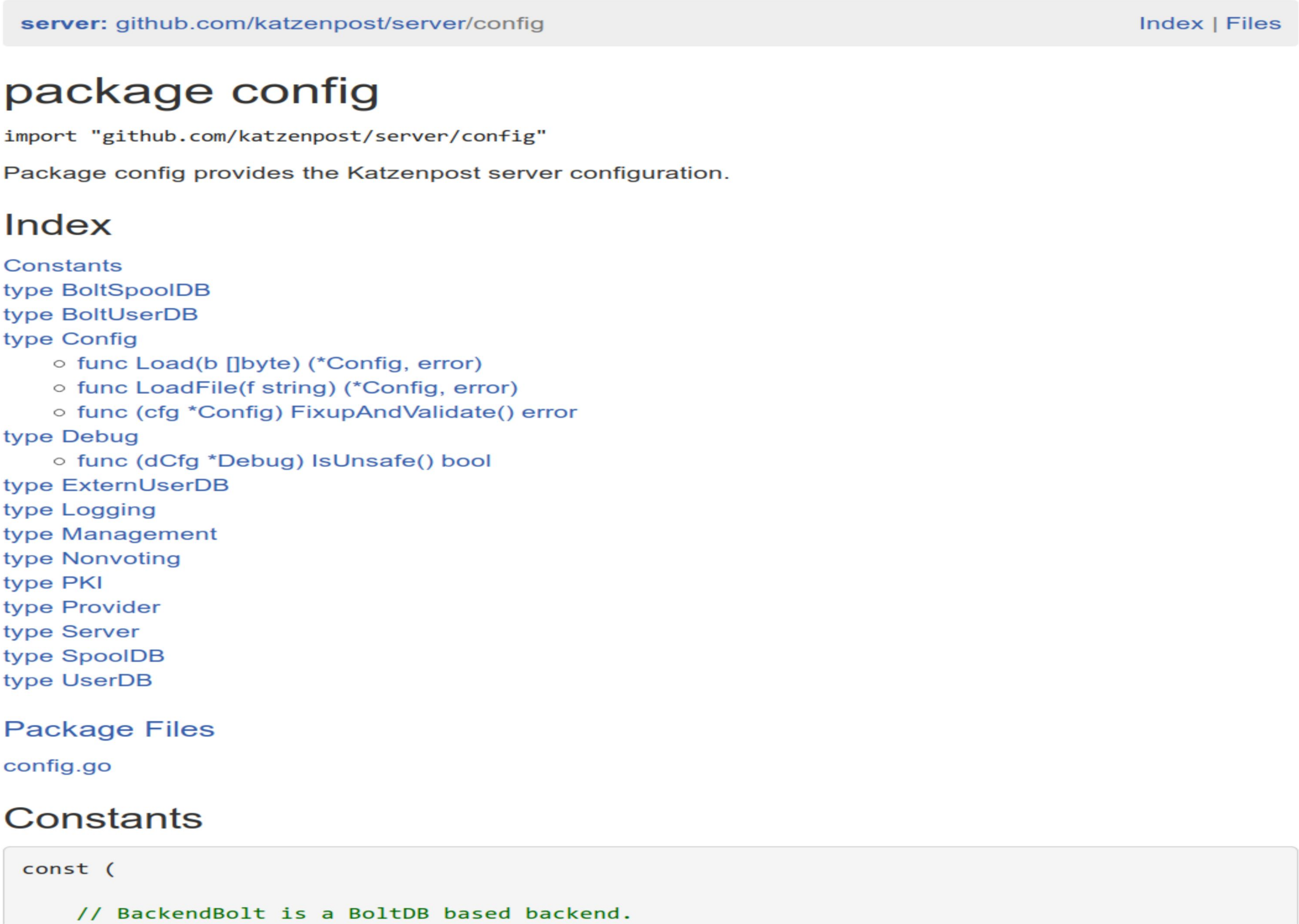
2 days ago

Build Jobs

✓	# 110.1		Go: 1.7	no environment variables set	1 min 12 sec
✓	# 110.2		Go: 1.8	no environment variables set	1 min 57 sec



github.com/katzenpost/core/sphinx 7 IMPORTS · 5 STARS	Package sphinx implements the Katzenpost parameterized Sphinx Packet Format.
github.com/katzenpost/core/constants 6 IMPORTS · 5 STARS	Package constants contains the constants for Katzenpost.
github.com/katzenpost/core/crypto/rand 5 IMPORTS · 5 STARS	Package rand provides various utitilies related to generating cryptographically secure random numbers and byte vectors.
github.com/katzenpost/core/crypto/eddsa 5 IMPORTS · 5 STARS	Package eddsa provides EdDSA (Ed25519) wrappers.
github.com/katzenpost/core/log 4 IMPORTS · 5 STARS	Package log provides a logging backend, based around the go-logging package.
github.com/katzenpost/server/userdb 4 IMPORTS · 1 STARS	Package userdb defines the Katzenpost server user database abstract interface.
github.com/katzenpost/core/wire 4 IMPORTS · 5 STARS	Package wire implements the Katzenpost wire protocol.
github.com/katzenpost/core/sphinx/commands 4 IMPORTS · 5 STARS	Package commands implements the Sphinx Packet Format per-hop routing info commands.
github.com/katzenpost/noise 3 IMPORTS · FORK · 2 STARS	Package noise implements the Noise Protocol Framework.
github.com/katzenpost/core/epochtime 3 IMPORTS · 5 STARS	Package epochtime implements Katzenpost epoch related timekeeping functions.



package config

`import "github.com/katzenpost/server/config"`

Package config provides the Katzenpost server configuration.

Index

Package Files

config.go

Constants

```
const (

    // BackendBolt is a BoltDB based backend.
```

Deployment (server-side)

- Configuration file and local testbed generator/test environment (kimchi)
- Ansible scripts for provisioning