Least Authority
PRIVACY MATTERS

ZKAPs – Zero Knowledge Access Passes

Enabling Privacy in Required Data Collection

Presented by: Liz Steininger, CEO & Managing Director at Least Authority

Overview

1. Who We Are
2. ZKAPs (the intro)
3. Our Use Case & Problem
4. How PrivateStorage Works
5. Adapting Privacy Pass
6. The Result - ZKAPs in Practice

01

Who We Are

Our Work

Least Authority is committed to building and supporting the development of usable technology solutions and ethical business practices to advance digital security and preserve privacy as a fundamental human right.

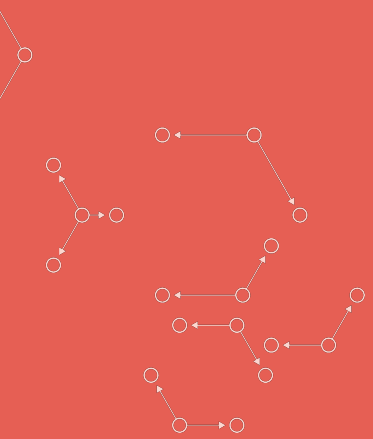
Security Consulting

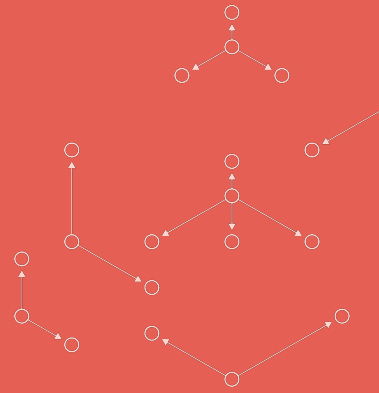
Product Development

Community-Contribution Projects

Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.

- Jerome Saltzer





02

ZKAPs (the intro)

What Are ZKAPs?

- ZKAPs = Zero-Knowledge Access Passes
- An anonymous, token-based authorization protocol
- A modified version of Privacy Pass <https://privacypass.github.io>
- Adapted to be used by PrivateStorage <https://privatestorage.io>

03

Our Use Case & Problem

Use Case: PrivateStorage & Tahoe-LAFS

PrivateStorage = hosted and managed version of Tahoe-LAFS

Tahoe-LAFS is an open source, distributed secure storage solution

Focus on Privacy by Design (data minimization) enabled by Security by Design

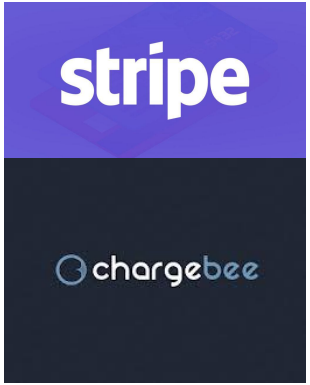
= storing data without collecting personal data

Problem: Required Data Collection

To process Fiat Currency payments, we need to collect personal data:

1. Name
2. Email address
3. Location (for VAT)
4. Transaction Data

And share it with these other companies:



= collecting personal data unnecessary for our service

04

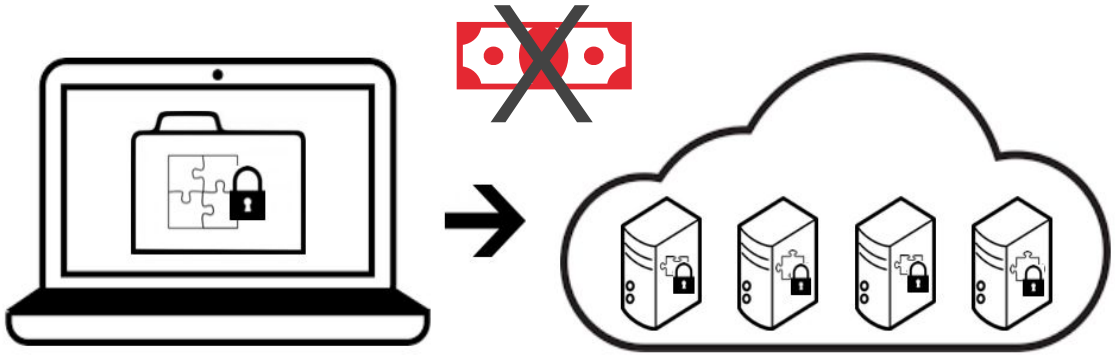
How PrivateStorage Works

Use Case: PrivateStorage & Tahoe-LAFS

- PrivateStorage, utilizing Tahoe-LAFS, has the following features:
  - Client-side encryption
  - Distribution of sharded ciphertext
  - Not ACL: No user accounts, no passwords
  - OCAP: Access based on possession of the capability string
  - This is also the decryption key

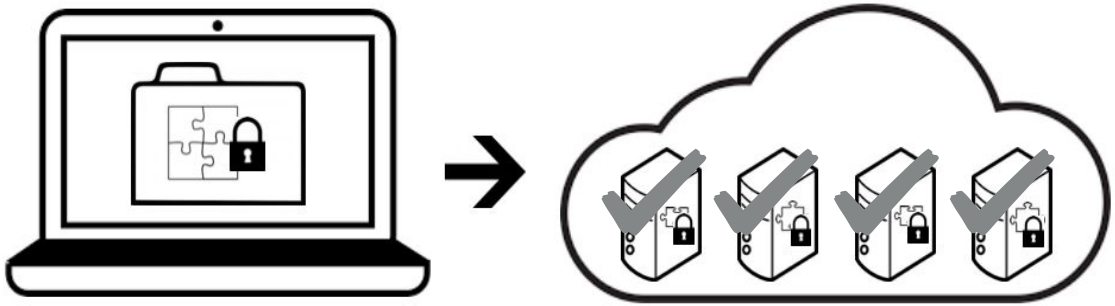
Use Case: PrivateStorage & Tahoe-LAFS

- Files and directories are encrypted on the client-side (locally)
- Shards of ciphertext get distributed on servers in a “grid”
- The Tahoe-LAFS protocol does not require money for this to happen



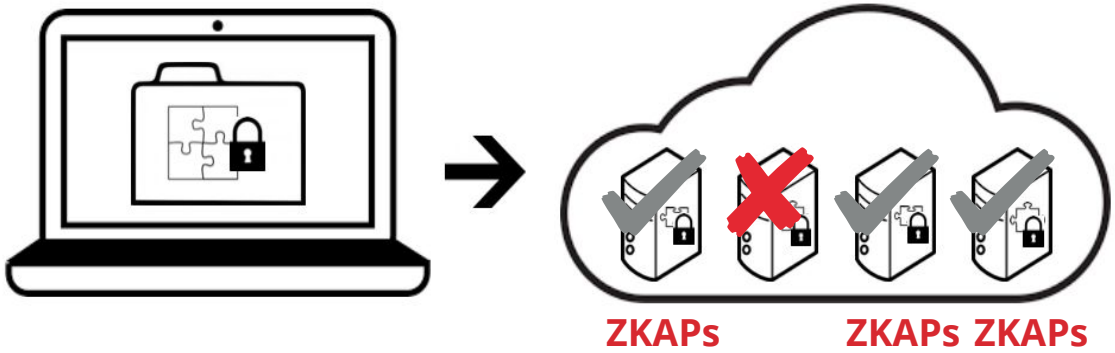
Use Case: PrivateStorage & Tahoe-LAFS

- No user accounts means a different approach to pay-for-storage
- Need a way to ensure that each shard being received is paid for
- The Tahoe-LAFS protocol includes leases on shards



Use Case: PrivateStorage & Tahoe-LAFS

- Modified the PrivateStorage storage servers to require ZKAPs
- The leases for shards are set based on the ZKAPs
- Without ZKAPs, the storage servers will not allow the shards to be stored



05

Adapting Privacy Pass

Privacy Pass: Cloudflare and Tor Browsing

- Problem:
  - Tor Browsers visiting Cloudflare (CDN) served pages looked like bots
  - Too many CAPTCHAs (proof-of-humanness) made it unusable
- Basic Solution Concept:
  - One action results in a batch of tokens
  - Tokens provide anonymity

Privacy Pass: History & Credit

- Idea based on Chaum's Ecash (1983)
  - You take a token, blind it, get a blind signature
  - Issuance and Redemption are unlinkable
- Privacy Pass: Bypassing Internet Challenges Anonymously (2018)
  - Batch of blinded tokens issued when a CAPTCHA is solved
  - Multiple tokens can be redeemed later, unlinkable by Cloudflare

Zero-Knowledge Cryptography

- Batched EC-VOPRF with redemption
  - Elliptic Curve (EC) - Verifiable Oblivious Pseudo-Random Function (VOPRF)
  - Verifiable only by the issuer at redemption
  - Batched validation for efficiency
- EC-VOPRFs use a Discrete Log Equivalence Proof
  - Short zero-knowledge proof
  - Two pairs of points have the same Discrete Log
  - Denounced **DLEQ(P:R == Q:S)**

Privacy Pass: Our Adaptation

- Proof-of-payment [not proof-of-humanness]
- Integrated with the Tahoe-LAFS protocol [not Cloudflare]
- Tokens (ZKAPs) redeemed for storage-time [not webpage access]
- Developed as a new/separate solution [not a browser extension]

06

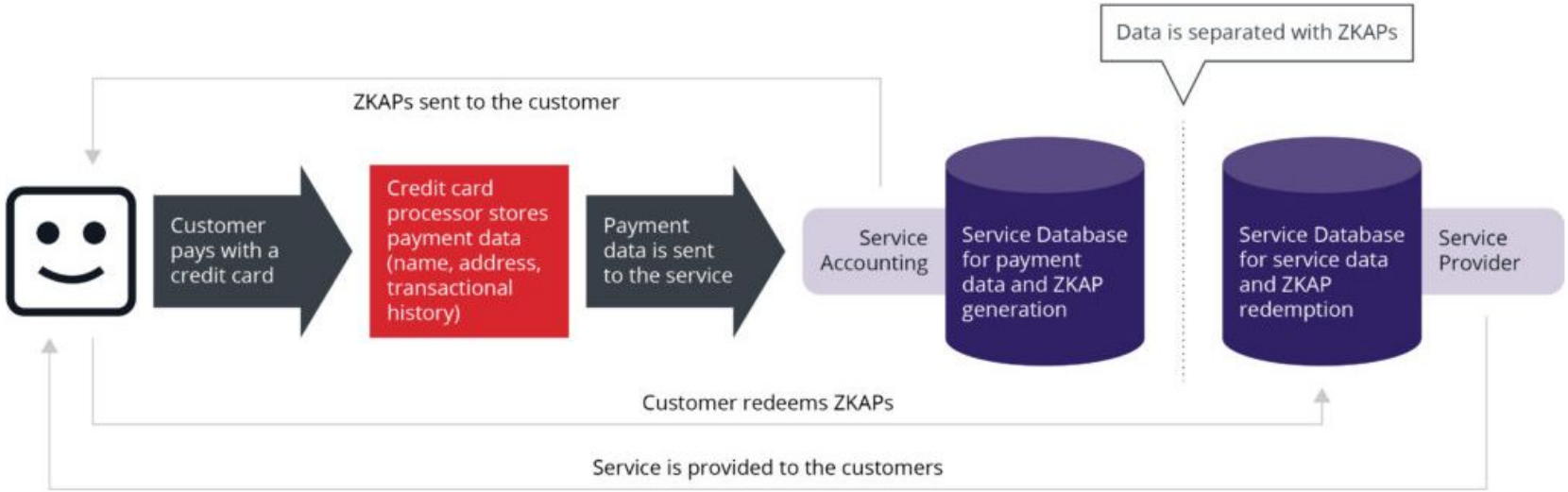
The Result – ZKAPs in Practice

How ZKAPs Work in Practice

- ZKAPs can be used to authorize individual actions without identifying individual users
- Uses batches of blind signatures as spendable “tokens”
- Usage: Spend X tokens to perform resource-limited action Y
    - e.g. (PrivateStorage): spend X ZKAPs to store X MBs for 1 month
- Tokens cannot be linked to token-holders or to each other
- Tokens cannot be forged; issuance is controlled

Less Privacy: Data Linkage without ZKAPs

How ZKAPs Help with Privacy

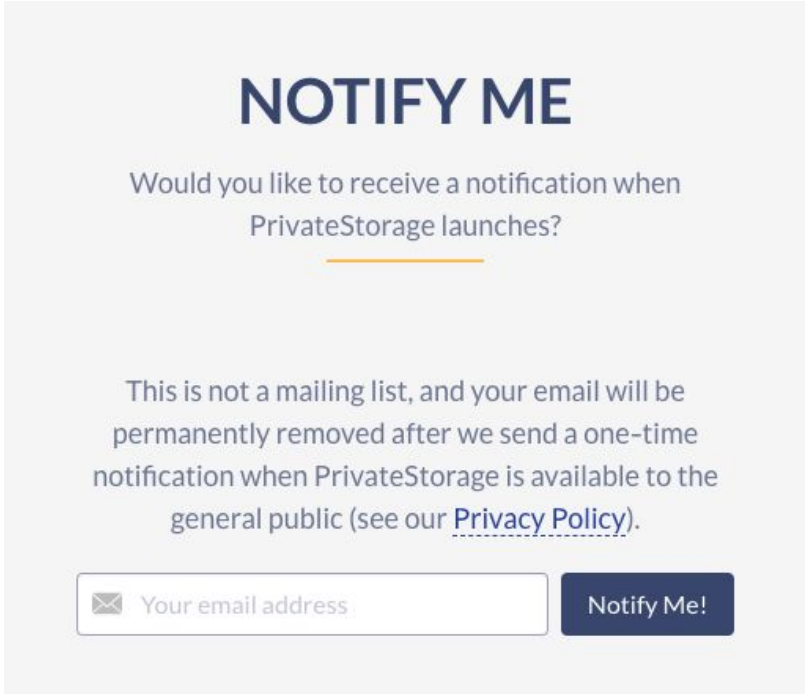


Expanding on ZKAPs Usage

- Different types and denominations of ZKAPs for Tahoe-LAFS
  - Proof-of-membership or proof-of-donation, instead of proof-of-payment
- Different services accepting different ZKAPs
  - Enabling privacy in more services
  - Potential for limited interoperability
- Secondary market for ZKAPs
  - Offers enhanced privacy

Other Potential Use Cases

- **Software-as-a-Service**
  - Where service does not need to be personalized
  - Could enable acceptance of anonymous users
  - Could enable creation of secondary market
  - Possible on-ramp to accepting cryptocurrencies
- **Blockchain and Protocol development**
  - ZKAP “tokens” are not on a blockchain
  - Could function as an additional access control infrastructure



ZKAPs in Action

- We will be launching PrivateStorage later this year!
  - Sign up to be notified at privatestorage.io
- We are investigating offering ZKAPs as a standalone service
  - Email us if you want to talk about using ZKAPs at contactus@leastauthority.com

Links & References

https://privatestorage.io

https://leastauthority.com/zkaps/

https://privacypass.github.io/

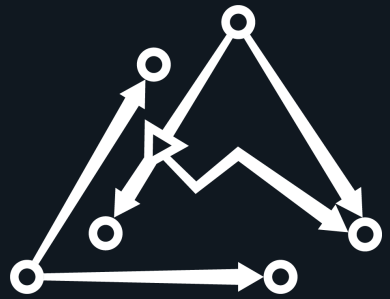
https://privacypass.github.io/protocol/

https://github.com/brave-intl/challenge-bypass-ristretto

https://github.com/LeastAuthority/python-challenge-bypass-ristretto

https://github.com/PrivateStorageio/ZKAPAuthorizer

https://leastauthority.com/blog/the-path-from-s4-to-privatestorage/



LEASTAUTHORITY.COM