Least Authority
PRIVACY MATTERS

A Real-World Case Study: Consulting Phreeli On Unlinkable Linkable Identifiers

10 May 2026

Poulami Das (poulami@leastauthority.com) &
Anna Kaplan (anna@leastauthority.com)

Real-World Case Study: Unlinkable Linkable Identifiers

unlinkable linkable

identifiers

Real-World Case Study: Phreeli

Phreeli is a phone service provider. They handle:

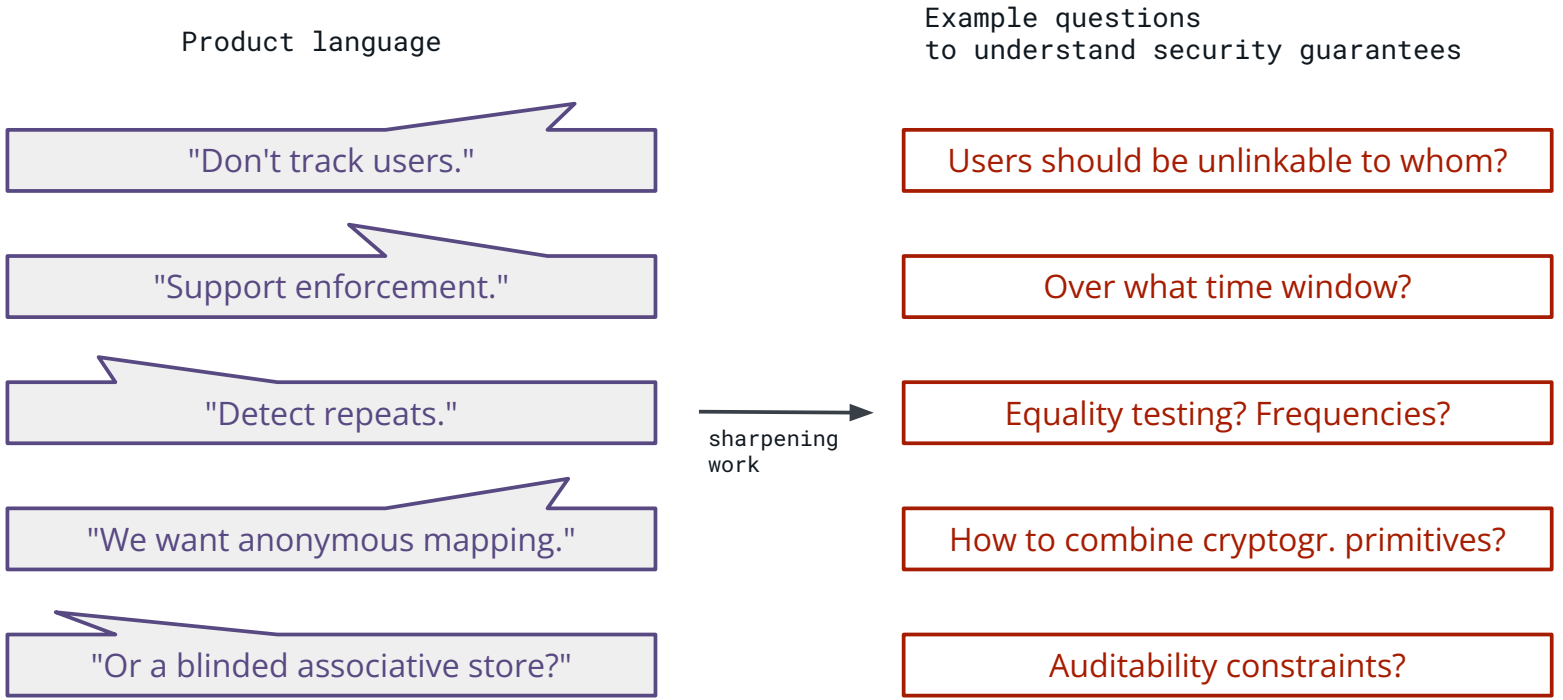
- eSIMs
- physical SIMs
- phone numbers
- etc.

But: They want their own customers to be as private as possible, **even from Phreeli itself**.

Not like the usual phone service provider!
(Picture generated by Claude)

Least Authority
PRIVACY MATTERS

Sharpening the Client's Objective



Sharpening the Client's Objective

Product language

"Don't track users."

"Support enforcement."

"Detect repeats."

"We want anonymous mapp

"Or a blinded associative st

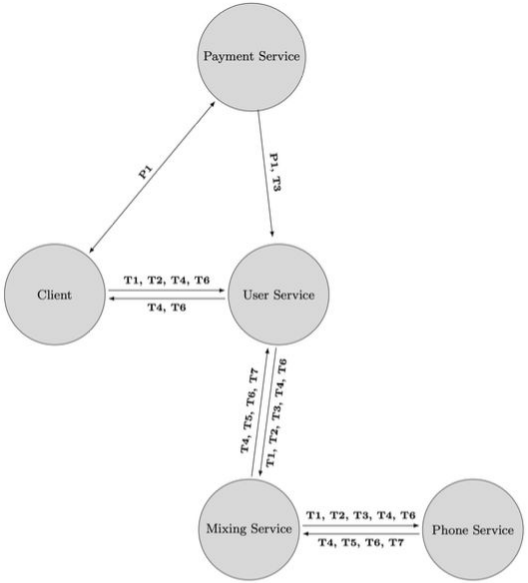


Figure 2: Simple Transactions Flow

Example questions
to understand security guarantees

hould be unlinkable to whom?

Over what time window?

iality testing? Frequencies?

combine cryptogr. primitives?

Auditability constraints?

Design and Engineering Concerns

Cryptographic primitives
(Example list)

- Fully-homomorphic encryption
- Multi-party computation techniques
- Matchmaking encryption
- Zero-knowledge proofs of all kinds
- Anonymous credentials, tokens, blind signatures

Design and Engineering Concerns

`Cryptographic primitives (Example list)`

- Fully-homomorphic encryption
- Multi-party computation techniques
- Matchmaking encryption
- Zero-knowledge proofs of all kinds
- Anonymous credentials, tokens, blind signatures

`Select/combine cryptographic primitives according to…`

… the client's main extracted **security guarantees**:

- Unlinkability of user ID and phone ID
- Abuse detection
- Chargeback possibility

… the client's **constraints**:

- Minimal engineering difficulty
- Minimal inter-server dependency

Design and Engineering Concerns

`Cryptographic primitives (Example list)`

- Fully-homomorphic encryption
- Multi-party computation techniques
- Matchmaking encryption
- Zero-knowledge proofs of all kinds
- Anonymous credentials, tokens, blind signatures

`Select/combine cryptographic primitives according to…`

… the client's main extracted **security guarantees**:

- Unlinkability of user ID and phone ID
- Abuse detection
- Chargeback possibility

… the client's **constraints**:

- Minimal engineering difficulty
- Minimal inter-server dependency

Design and Engineering Concerns

`Cryptographic primitives (Example list)`

- Fully-homomorphic encryption
- Multi-party computation techniques
- Matchmaking encryption
- Zero-knowledge proofs of all kinds
- Anonymous credentials, tokens, blind signatures

`Select/combine cryptographic primitives according to…`

… the client's main extracted **security guarantees**:

- Unlinkability of user ID and phone ID
- Abuse detection
- Chargeback possibility

… the client's **constraints**:

- Minimal engineering difficulty
- Minimal inter-server dependency

`Security engineering factors (Example list)`

- Timing attacks
- Key custody
- Rate limits
- Metadata
- Monitoring

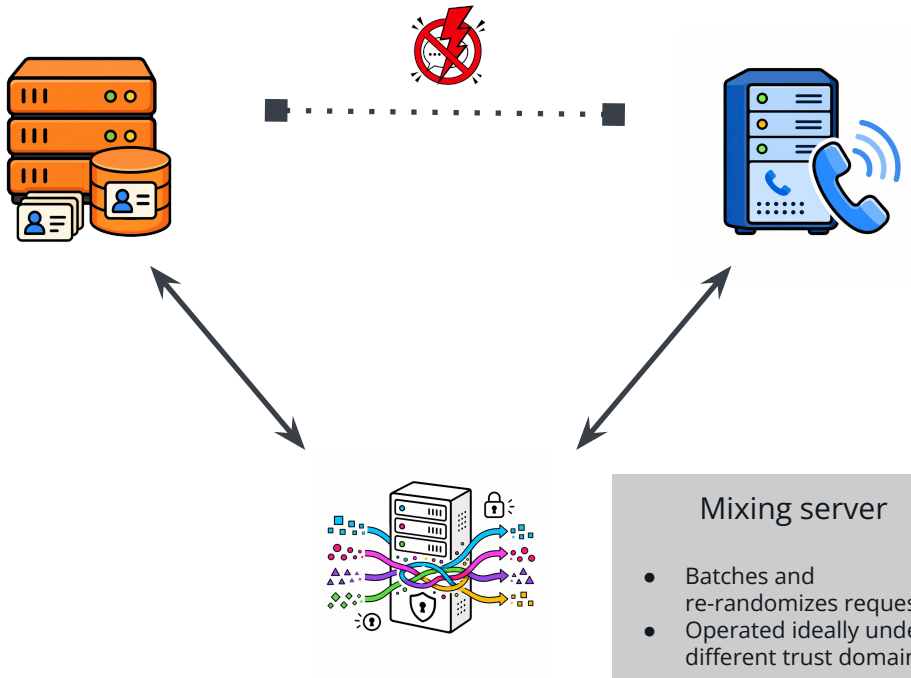
The Architecture We Landed On

User server

Handling all user-related information, e.g.:

- Creating account
- Including payment methods
- Updating contact details

"knows the customer"



Phone service server

Handling phone service transaction, e.g.:

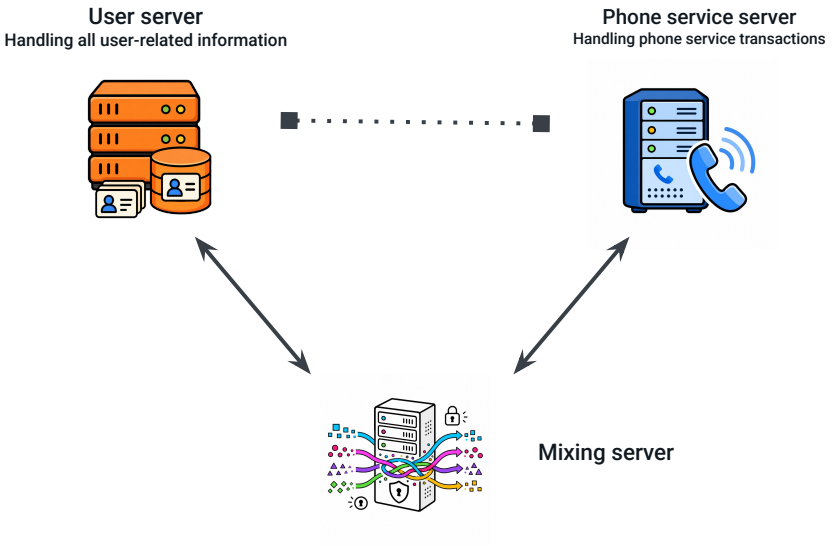
- Provisioning a SIM
- Activating a number
- Configuring it on the network
- Handling top-ups

"knows the eSIM/SIM number"

Mixing server

- Batches and re-randomizes requests
- Operated ideally under a different trust domain

One Step towards a Solution

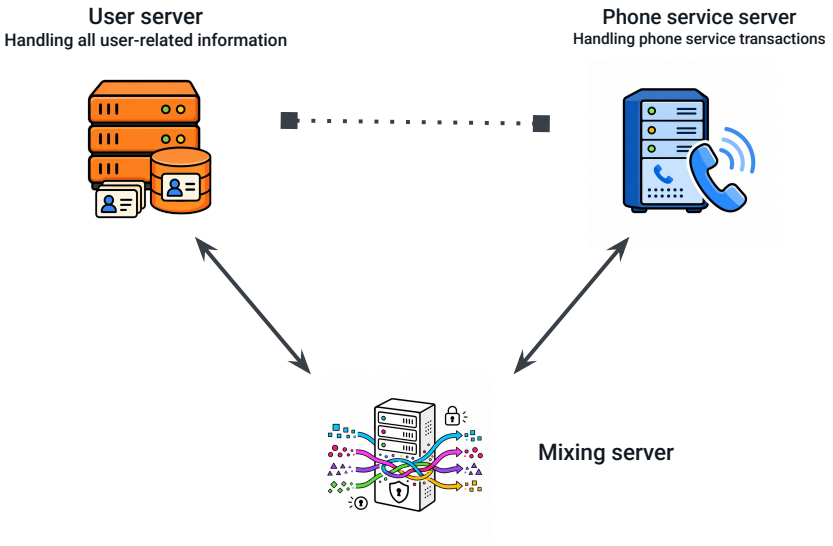


Two main security/privacy properties that capture Phreeli's requirements:

- User authentication:

- User ID to Phone ID unlinkability:

One Step towards a Solution



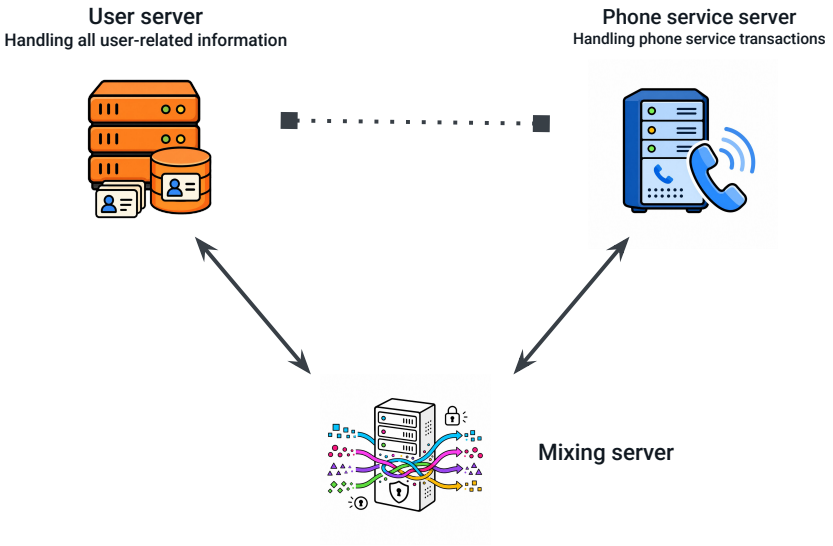
Two main security/privacy properties that capture Phreeli's requirements:

- Anonymous token-based authentication:

  Privacy Pass

- User ID to Phone ID unlinkability:

One Step towards a Solution



Two main security/privacy properties that capture Phreeli's requirements:

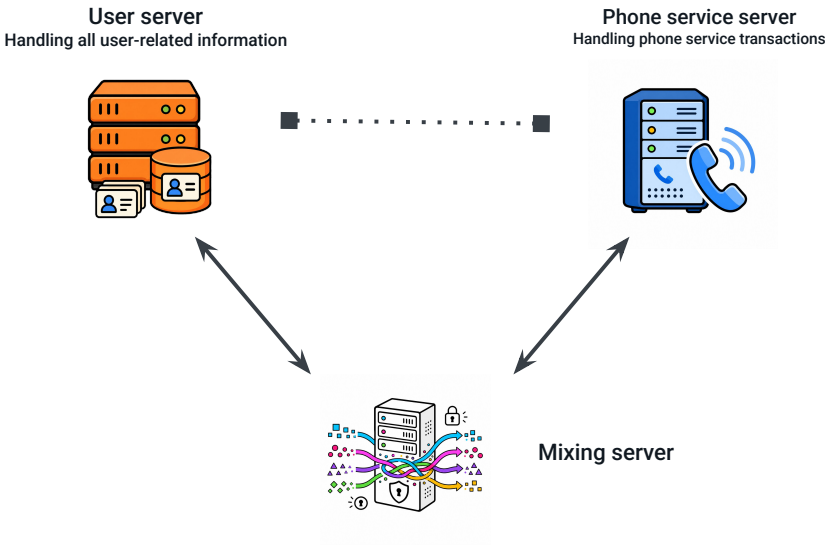
- Anonymous token-based authentication:

  Privacy Pass

- User ID to Phone ID unlinkability:

  (Trusted) Mix service

One Step towards a Solution



Two main security/privacy properties that capture Phreeli's requirements:

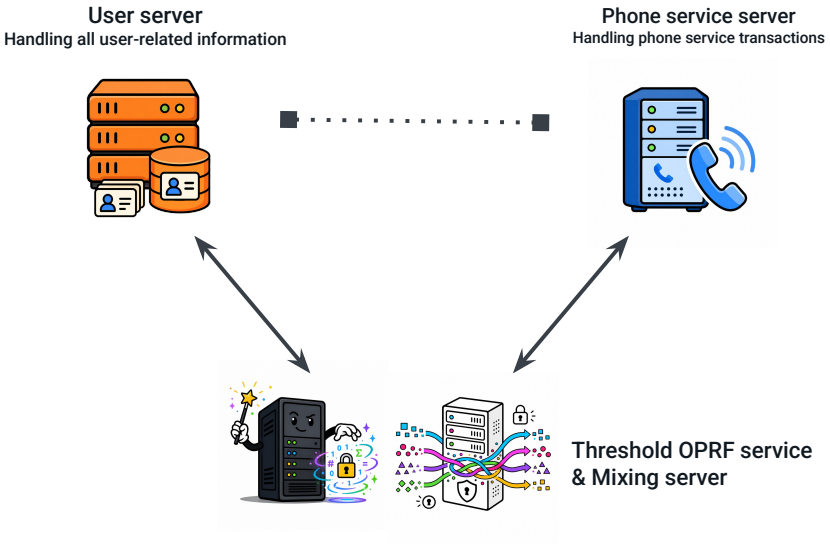
- Anonymous token-based authentication:

  Privacy Pass

- User ID to Phone ID unlinkability:

  (Trusted) Mix service

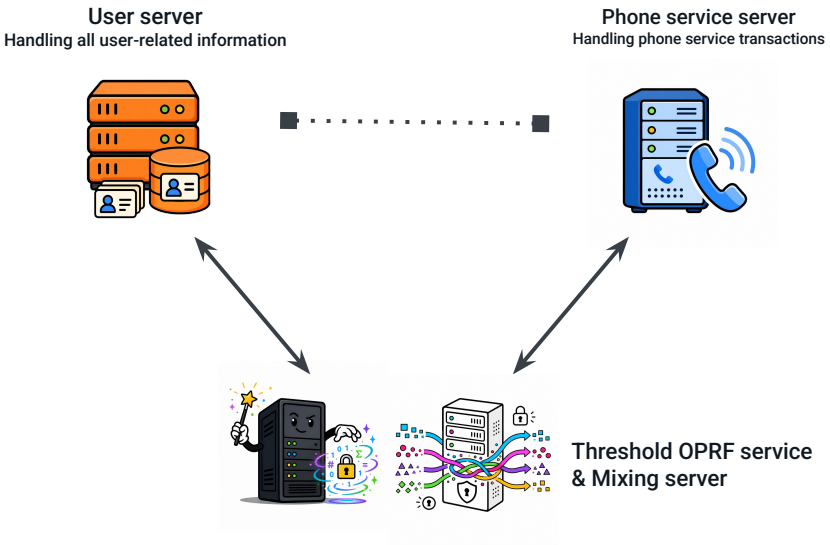
Towards a Better Solution



User ID to Phone ID unlinkability:

- Threshold Oblivious PRF
- Hybrid PKE

Threshold OPRF + HPKE: Overview



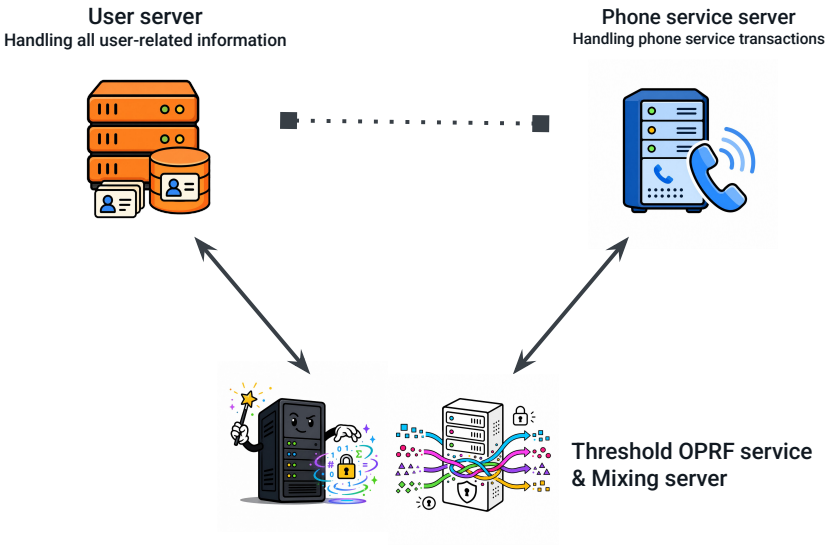
User ID to Phone ID mapping:

- Mapping creation: `<val1, val2>`
  - `u = Hash(user_ID || n)`
  - `v = TOPRF(u)`
  - `val1 = Hash(v)`
  - `val2 = Enc(phone_ID)`
- Store `<val1, val2>` in Mix service
- Mapping lookup (similar flow)

Phone ID to User ID mapping:

- flow in the opposite direction

Why does this work?



- **Threshold** property of TOPRF
  - Servers shared among LA + Phreeli
- **Pseudorandomness** of the TOPRF output
- **Obliviousness** of the TOPRF input

Conclusion

- Further improvement possibilities:
  - User service - Phone service collusion
  - Support encrypted payloads
  - Post-quantum security

- Reference for our TOPRF solution:
  - *Stanislaw Jarecki, Aggelos Kiayias, Hugo Krawczyk, Jiayu Xu:*
    TOPPSS: Cost-Minimal Password-Protected Secret Sharing Based on Threshold OPRF.
    ACNS 2017

Thank you for listening!

Please contact us if you have more questions!

Poulami: poulami@leastauthority.com | Anna: anna@leastauthority.com