

# OZKi

## Proof Framework

### What is OZKi?

OZKi (Open Zero Knowledge Integration) is a zk-SNARK based proof framework for developing privacy protecting components of a web application using verifiable computation as its underlying technology.



# 71%

The Verizon Data Breach Investigations Report noted that 71% of the data compromised within the Financial sector was Personal data.

# 44%



According to IBM customer personally identifiable information (PII) was included in 44% of breaches in 2021.

**OZKi** is designed to help web application developers implement



## Privacy-Protecting



features with minimal efforts.

## Why OZKi?

### INNOVATIVE

Unique proof tooling for webapp development.

### EASE OF USE

Offers flexibility and simplified integration for web applications.

### SECURE PII RETRIEVAL

Adds additional layers of security on top of the core ZKP system.



### USEFUL FEATURES

Proof of Payment with PayPal, Proof of Login with Google, Proof of Key, etc.

### OPPORTUNITY

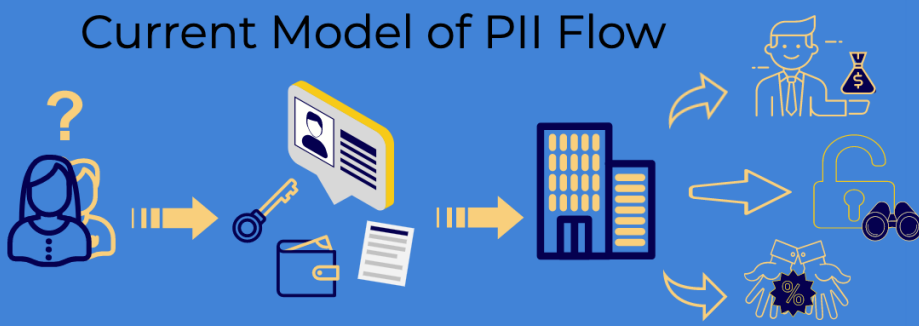
Building block for Proof-As-a-Service business opportunities.

### PERFORMANT

OZKi processing typically completes under 2 seconds.

The user is typically asked to submit a lot of personally identifiable information, many of which are not really needed, to the server.

### Current Model of PII Flow



The average total cost of a data breach was \$4.24 million in 2021.

### OZKi-enabled PII Protection Model



**Proof**

The proof reveals only information whether the PII meets certain constraints or requirements



The user never sends the PII to the server. Instead of PII, the user sends only a proof.

### SOURCES

[www.comparitech.com/](http://www.comparitech.com/)  
Verizon DBIR 2022  
IBM CoD Breach Report 2021

### OZKi Online Book

<https://vizualkei.gitbook.io/ozki>



### MICS-OZKi

GitHub is where  
MICS-OZKi builds...  
[github.com](https://github.com)