

WHITE PAPER



# PRAMAAN

Zero Knowledge Based  
Authentication

# Table of Content

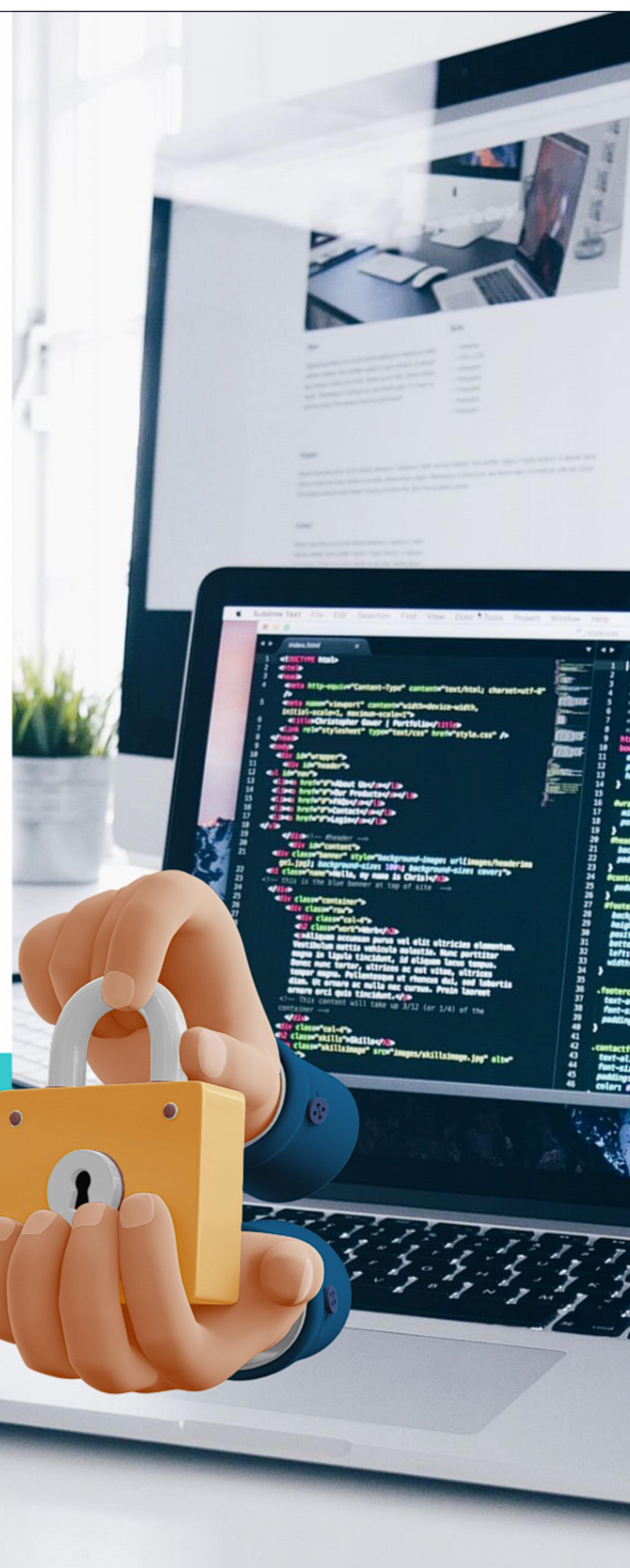
- |    |                          |
|----|--------------------------|
| 01 | Overview                 |
| 02 | <b>What is Pramaan?</b>  |
| 03 | Why do we need Pramaan?  |
| 04 | <b>How does it work?</b> |
| 05 | Architecture             |
| 06 | <b>The Impact</b>        |
| 07 | Vision for the Future    |
| 08 | <b>Our Team</b>          |

# Overview

Pramaan is a revolutionary web authenticator developed by Yushu Excellence Pvt Ltd. It provides a zero-knowledge proof protocol that ensures user privacy and security.

With Pramaan, users can authenticate themselves without revealing any personal information, eliminating the need for traditional passwords.

Pramaan enables seamless and secure access to web services, safeguarding sensitive data from unauthorized access. Experience a new era of authentication with Pramaan, where privacy and security are prioritized without compromising user convenience.



# What is Pramaan?

---

Pramaan, developed by Yushu Excellence, is a groundbreaking zero-knowledge-based web authenticator. By leveraging advanced cryptography techniques, Pramaan ensures utmost privacy and security for users. It operates by taking an individual's identification (ID) as input and generates a unique identifier (UID) without storing or transmitting any personal information. This innovative approach eliminates the need for traditional authentication methods that rely on passwords or biometrics, reducing the risk of identity theft and unauthorized access. With Pramaan, users can securely access web services without compromising their privacy. Embrace the future of authentication with Pramaan, where your identity remains confidential, and your online experiences are protected like never before.



# Why do we need Pramaan?

---

## Enhanced Privacy and Security:

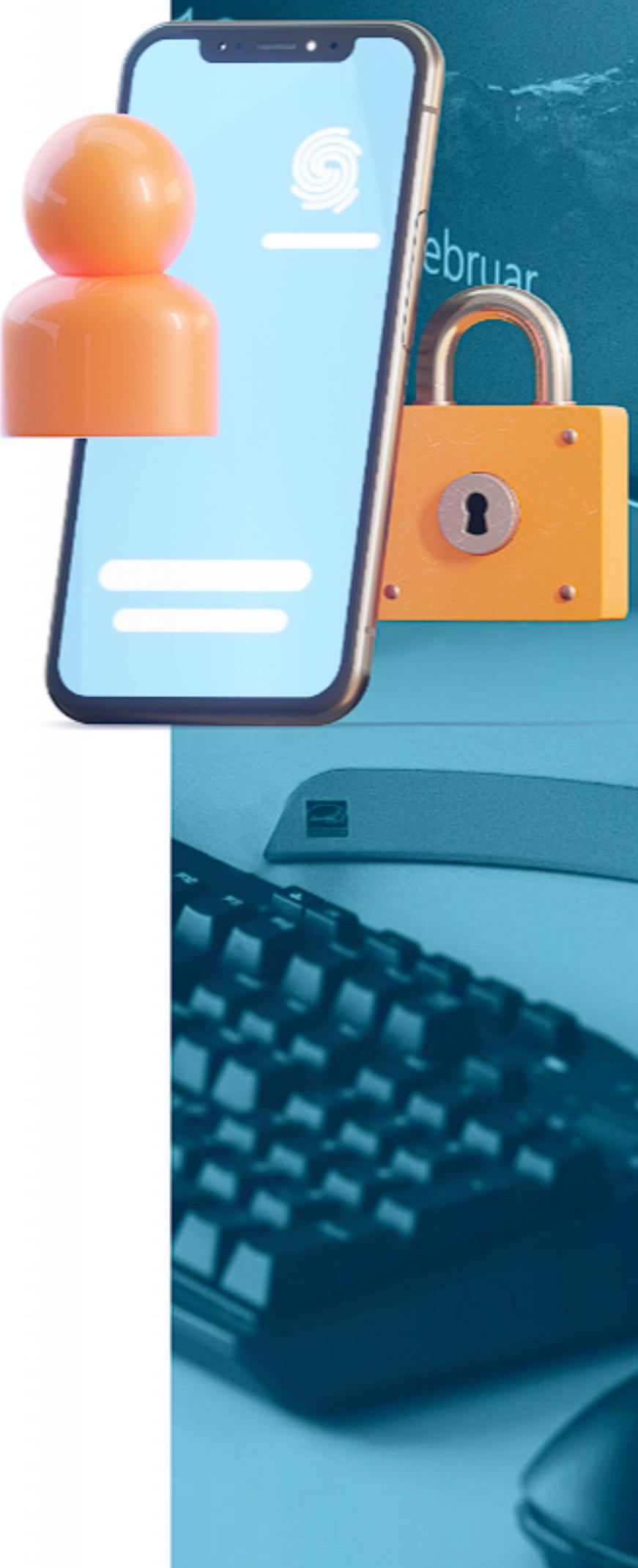
- Utilizes zero-knowledge proof protocol to authenticate without revealing personal information.
- Minimizes the risk of data breaches and identity theft.
- Protects user privacy by ensuring sensitive information remains confidential.
- Reduces the potential impact of a breach by not storing personal data.

## Protection of Sensitive Data:

- Generates unique identifiers (UIDs) instead of storing personal information.
- Minimizes the exposure of sensitive data to potential threats.
- Safeguards against unauthorized access to personal details.
- Mitigates the risk of data leakage even in the event of a system compromise.

## Future-Proof Authentication:

- Adapts to evolving security needs and technologies.
- Offers a robust and scalable solution for authenticating users.
- Supports seamless integration with various web services and platforms.
- Provides a foundation for secure and reliable user authentication in the digital age.



# How does Pramaan Works

---

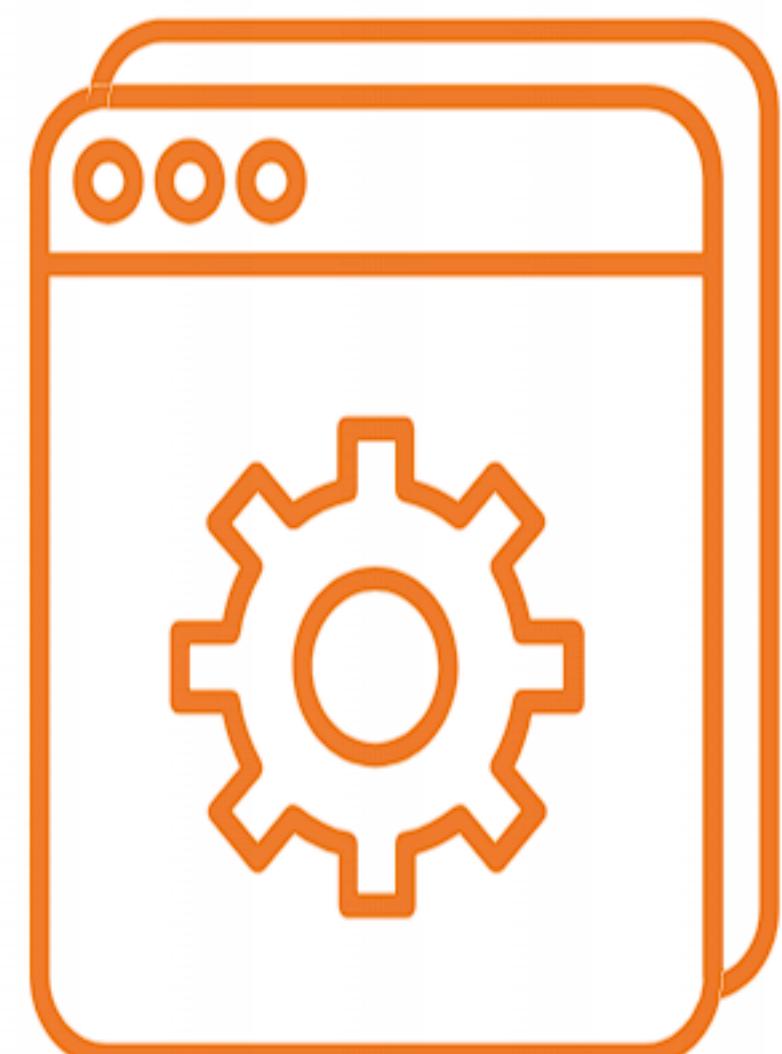
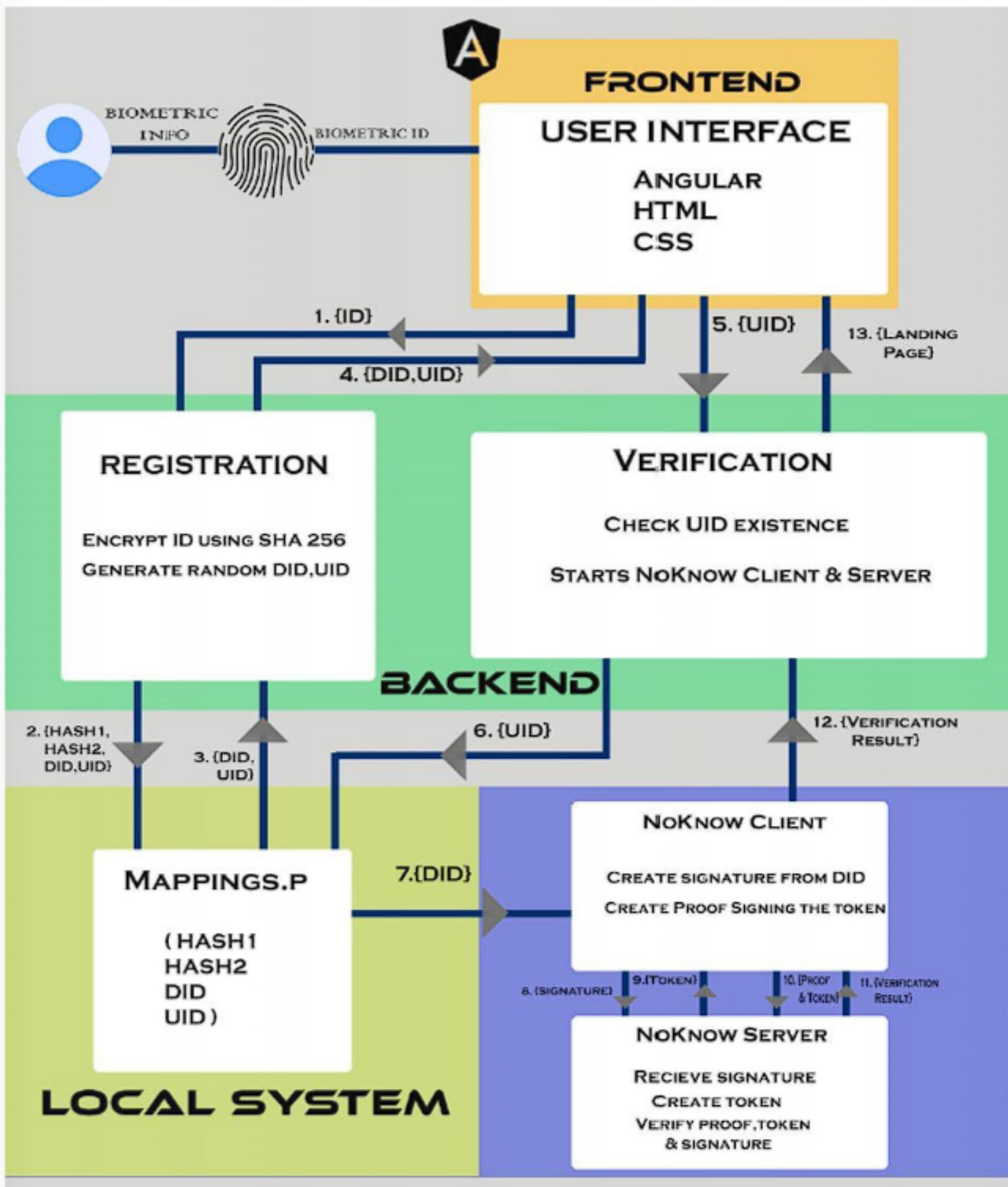
Pramaan operates through a series of steps to ensure secure and privacy-preserving authentication. Here's an overview of its working:

1. Input: Pramaan takes an identification (ID) from the user as input.
2. Hash Generation: The ID is processed to generate two unique hashes, Hash1 and Hash2. These hashes serve as cryptographic representations of the ID, ensuring the original ID remains hidden.
3. DID Generation: Pramaan generates a Decentralized Identifier (DID) using the generated Hash1 and Hash2. The DID acts as a unique identifier for the user, allowing them to be recognized without revealing their actual ID.
4. UID Generation: Pramaan further generates a unique identifier (UID) associated with the user. The UID is a cryptographic representation of the user's identity, ensuring privacy and confidentiality.
5. UID Transmission: The UID is securely sent to the user, usually through a secure channel or encrypted communication.
6. Zero-Knowledge Proof (ZKP): When the user needs to authenticate, they present the UID to the system. Pramaan utilizes the Noknow library in the backend to perform a zero-knowledge proof (ZKP). The ZKP verifies the authenticity of the user without revealing any sensitive information about their identity.
7. Authentication: If the ZKP is successful, the user is granted access to the desired web service or platform, ensuring a secure and privacy-preserving authentication process.

In summary, Pramaan combines hashing techniques, unique identifier generation, and zero-knowledge proofs to enable secure and private authentication while protecting user identities from unauthorized disclosure.



# Architecture:



# The Impact:

---

## Efficient and Convenient Authentication:

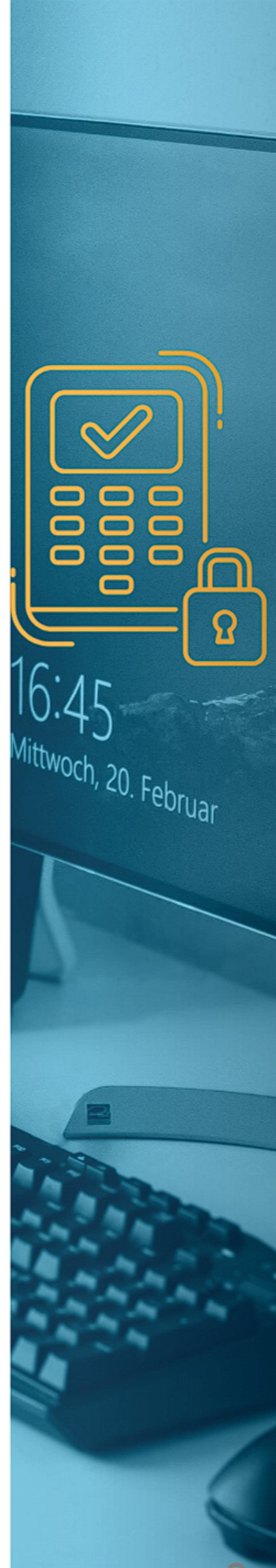
- Eliminates the need for traditional passwords, reducing the burden of password management for users.
- Offers a seamless and hassle-free authentication experience with quick and secure access to web services.
- Enhances user convenience by simplifying the authentication process, saving time and effort.
- Streamlined user experience leads to increased user satisfaction and engagement.

## Reduction in Identity-Related Risks:

- Minimizes the reliance on personally identifiable information (PII) for authentication, reducing the risk of PII-related attacks.
- Protects against identity fraud and impersonation attempts by utilizing cryptographic representations and secure protocols.
- Diminishes the chances of password-related vulnerabilities and brute-force attacks.
- Provides a robust defense against account takeovers and unauthorized access attempts.

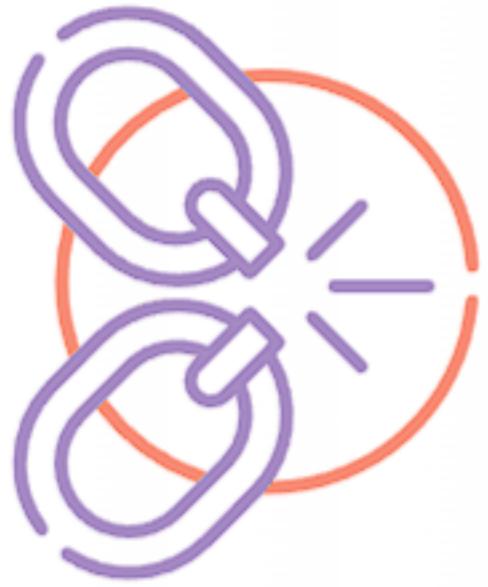
## Future-Proof and Scalable Solution:

- Pramaan is designed to adapt to evolving security needs and technologies.
- Offers scalability and compatibility with various web services and platforms.
- Provides a foundation for secure and reliable user authentication in the digital age.
- Promotes the adoption of zero-knowledge proof protocols and privacy-enhancing technologies.



# Vision For The Future

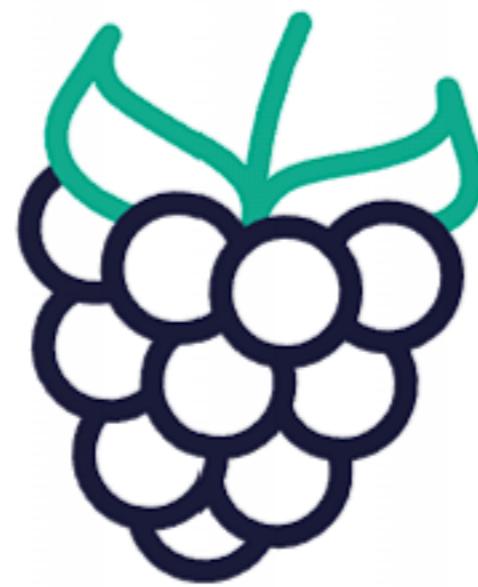
---



Blockchain  
Integration



Cloud  
Deployment



IoT  
Deployment

# Our Team:

---



**Mr. Amulya Gupta**



**Dr. Amit Dua**



**Mr. Arijet Sengupta**



**Mr. Garvit Sharma**



**Ms. Ipshita Mahapatra**