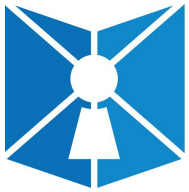


Journey

The Trusted Identity Platform

# Zero Knowledge Identity

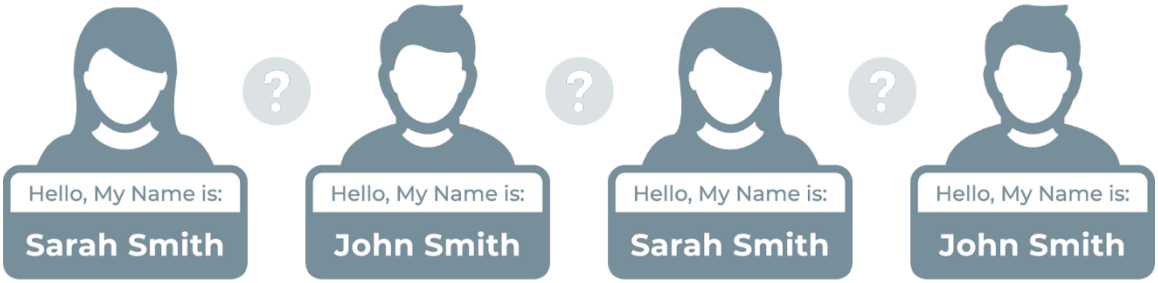
## Protecting Private Information and Building Digital Trust

06/10/2020

Sorell Slaymaker

# Introduction

Identity management is the foundation of the new Digital Enterprise, and superb identity management is the foundation of strong security. The establishment and usage of identities supports virtually every application and process throughout any organization. The management of identities is also a critical part of how organizations directly interact with customers and partners. Too many security solutions fail to stop impersonation, and once someone's identity is compromised, fraud occurs.




**Who Are the Real John & Sarah Smith?**

As enterprises accelerate their Digital Enterprise programs, identity management is crucial to the success in properly securing, orchestrating, and managing enterprise interactions. Identity should ultimately be a "utility" to easily identify individuals, applications, and things, as well as provide access under proper security controls that are privacy-centric.

Zero Knowledge Identity (ZKI) allows for data to be shared between two parties without the use of a password or any other information associated with the transaction. As a result, no information, either from the sender's or receiver's end, can be compromised in any way. This is quite useful, especially because such a level of safety provides an avenue to communicate with one another without having to reveal the content of interactions with any third party. A subset of this is Zero Knowledge Proofs which allow a person to prove a claim about themselves without having to reveal all the details of that claim.

Zero Knowledge Identity is the next iteration of identity services that will empower enterprises to achieve:

> **Digital Transformation** – Drive business growth by integrating secure and seamless user experiences while giving end users more control.

**Zero Trust Delivery** – Knowing the right users under the right conditions have the right access to the right applications and data.

**Compliance Insurance** – Getting ahead of regulatory mandates and company audits while reducing enterprise risk.

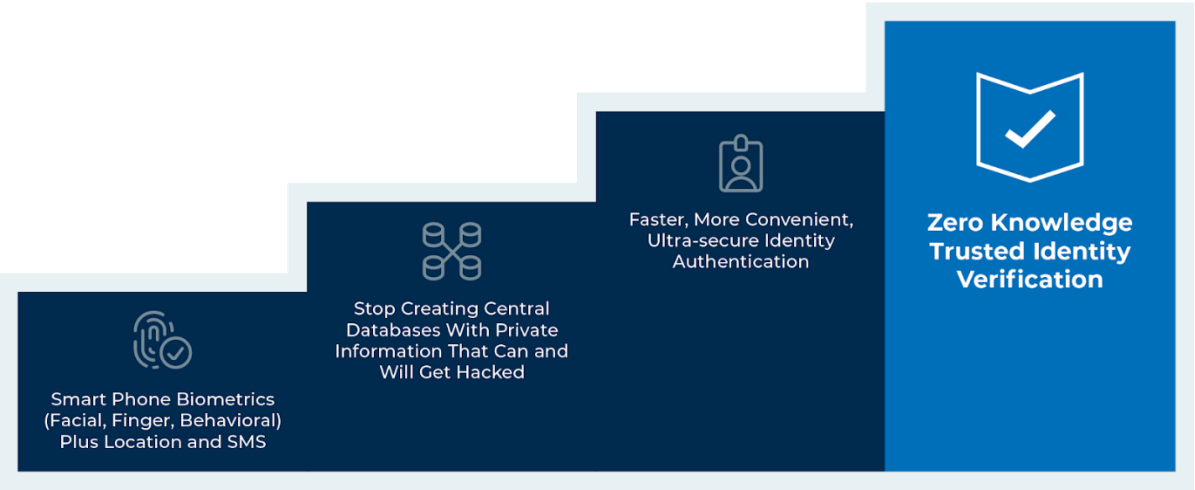
**Reducing Risks** – Removing the value of hacking by storing less private information, and for information that is stored, it is done so in a distributed manner which removes single points of vulnerability.

## Why Now?

Identity systems continue to evolve. We started with centralized identity, which lives within a single organization and was hierarchical and directory- and object-based. Next came federated identity which reused identity across cooperative organizations where trust was rooted and verification depended on a single identity provider. The latest is decentralized identity where users own, store, and present attested data through interactions where trust is rooted in a decentralized system (ledger).

Evolving technology that enables a decentralized system:

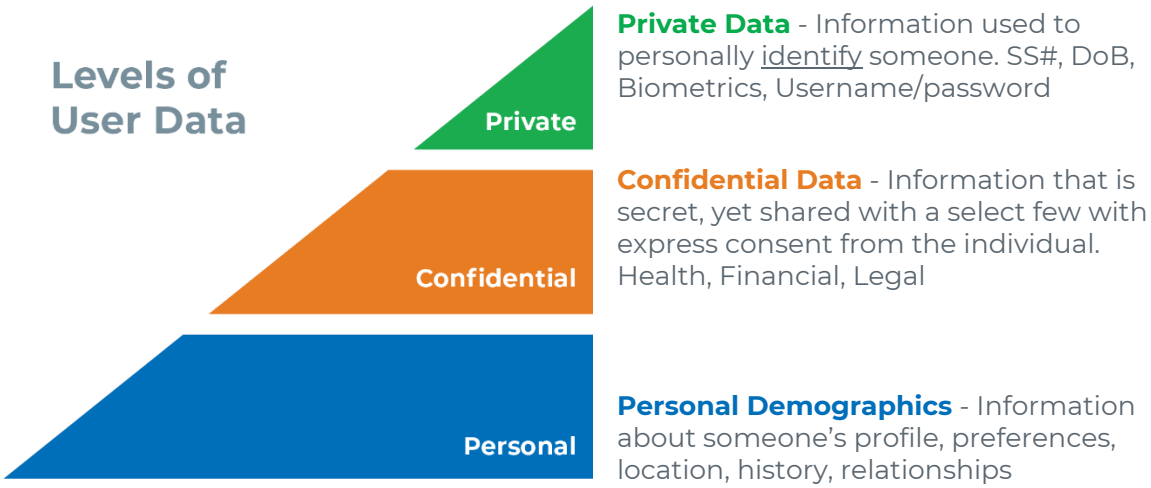
- Off-the-shelf devices – smart phones everywhere used by everyone
- Additional biometric capabilities – Facial, Behavioral
- New standards and capability – Distributed Identity, Zero Knowledge Proofs
- Convenient - Not having to remember unique passwords



Zero Knowledge systems no longer require security that requires users to remember passwords and additional questions regarding things like mother's maiden name which is irritating for users and does not provide a high level of security. Biometrics plus location and mutual authentication can provide a higher level of digital trust in a way that is quick and easy.

## Securing Private Information

Privacy is more important than ever with increased regulations such as GDPR and enterprise liability. Users want personalized and customized service without sharing their private data. There is an unspoken contract between businesses of what they can obtain and how they use and store this information. Too many enterprises store all customer data the same way and do not delineate various types of user data. **The solution is simple: If private data is never collected and stored, it cannot be stolen.**




As shown in the graphic above, there are different level of user data that need to be treated with different levels of security. The beauty of Zero Knowledge digital trust systems is that the private information is not collected or stored.

## Introducing Journey's Trusted Digital Identity Solution

Journey is a security business with the mission of making it simple for businesses to build trusted digital relationships with their customers

that deepen and grow in scope throughout the lifetime of their customer journey. The beauty of Journey's solution is that it blends security, privacy, simplicity into a single platform that enterprises can easily add to their digital systems.

**Security –** Customer data is prone to being stolen since the Internet was created without an identity layer and security has been something that has been bolted onto enterprise applications


**Privacy** – Customer data within the enterprise is treated like any other data they own and has only recently become an external customer trust and regulatory issue with all of the frequent data breaches and new privacy regulations like GDPR and CCPA.

**Customer Experience** – Customer experience normally deteriorates as you ratchet up security and privacy. The digital marketing industry describes this as the tradeoff between fraud and friction.

Journey's platform is a fundamentally new approach that ensures privacy and security while making it simple and easy for enterprises and the customers to use.

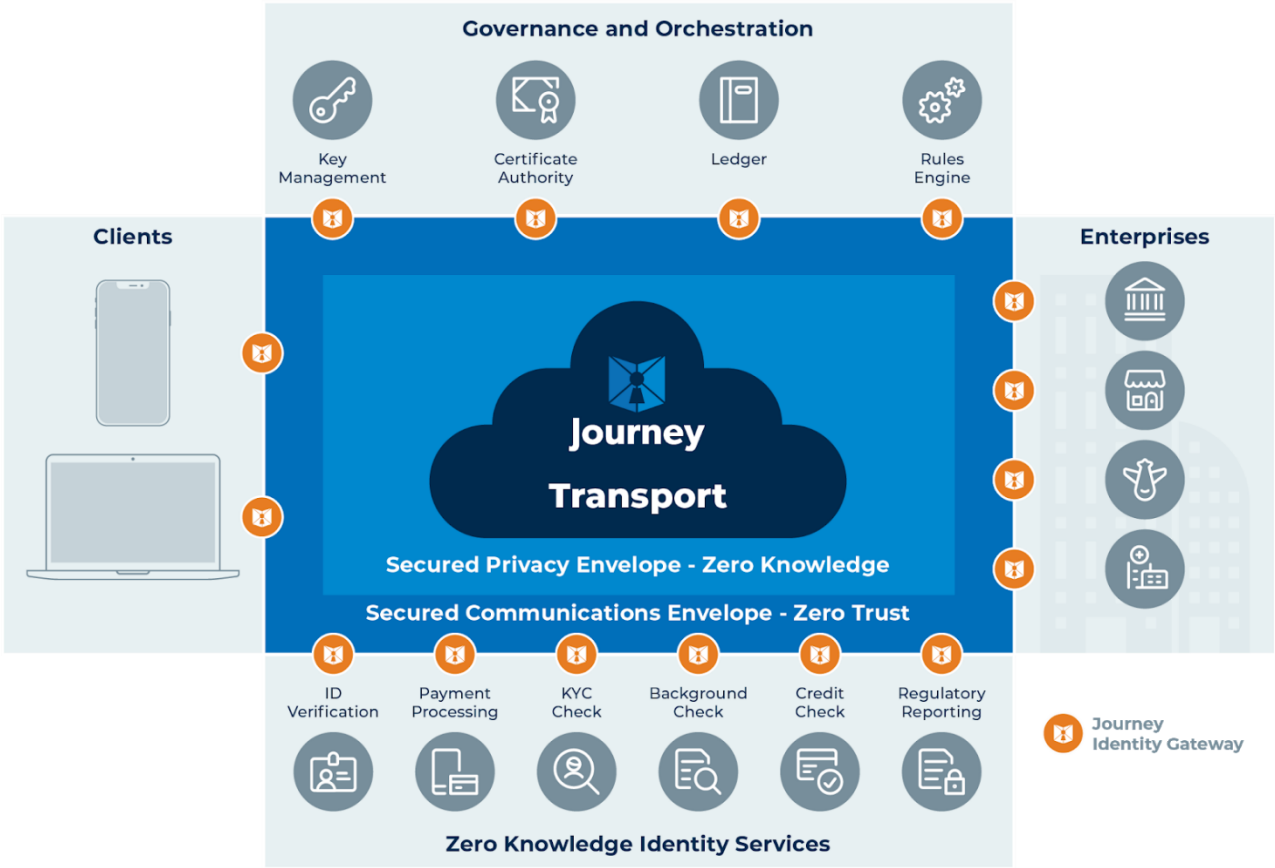
## A Trusted Digital Identity Solution

Mutual verification is the process of a customer and business asking one another, "Who are you?" Crossing the threshold from unknown to known is critical in building mutual trust and verification for interactions and transactions. The better you know someone, the better the conversation and experience. For instance, we use Uber where as the driver and the passenger do not know each other, but through the application and social experience, there is a level of trust. This trust is built without sharing private information.

Journey is a security business focusing on building trusted digital relationships between businesses and their customers. Journey addresses these challenges with the introduction of the **Zero Knowledge Identity Network** *(patent pending*). This new approach is based on the latest in cryptography, multi-tenant cloud orchestration and scaling technologies. It is also a streamlined process which virtually

eliminates friction in the customer experience while dramatically improving security and privacy. A few key attributes include:

- **High Veracity Biometric Authentication** – Authenticating a person independent of the device they are using nor having to share passwords
- **Zero Knowledge Verification** - Allows enterprises to verify customer identity and information, or complete transactions on the phone, through a chat or in-person without ever seeing customers' private data - personal, financial, or healthcare data.
- **Zero Trust Network** - Uses individually encrypted ephemeral sessions and never stores customer data or cryptographic keys, eliminating the typical honeypots of data that exist today and destroying hacker economics.
- **Distributed** – A distributed architecture with no single point of failure or vulnerability by utilizing many factors of authentication to be able to prove someone's identity with 10x more certainty than current solutions.



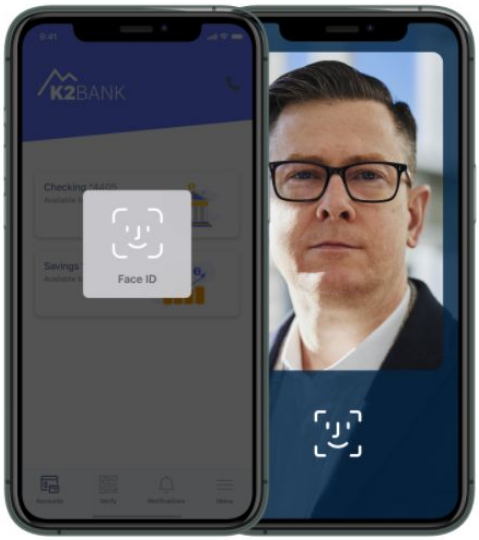
Users and clients on the left side need to communicate with services, applications, and data hosted on by enterprises on the right side. To facilitate this communication, the Zero Knowledge Identity services are leveraged at the bottom while being managed by the services at the top. Zero Trust and Zero Knowledge

# Use Cases of the Journey Trusted Digital Identity Platform

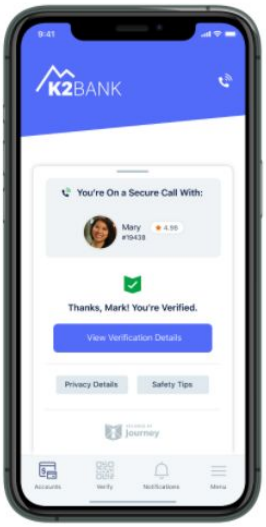
## Case #1 – Contact Center Verification of Trust

Verify Identity and authenticate your customers in seconds, rather than minutes, and provide instant rapport with mutual authentication. Now more than ever, customers value businesses who value their security, privacy and time. And they will reward you with their business. In the below example, a user gets an in-call notification, uses the biometrics available on the mobile phone along with other identity stores, and then connects the customer and agent in a mutually verified communication.


In-Call Notification




Built in Biometrics and/or 3rd Party Biometrics

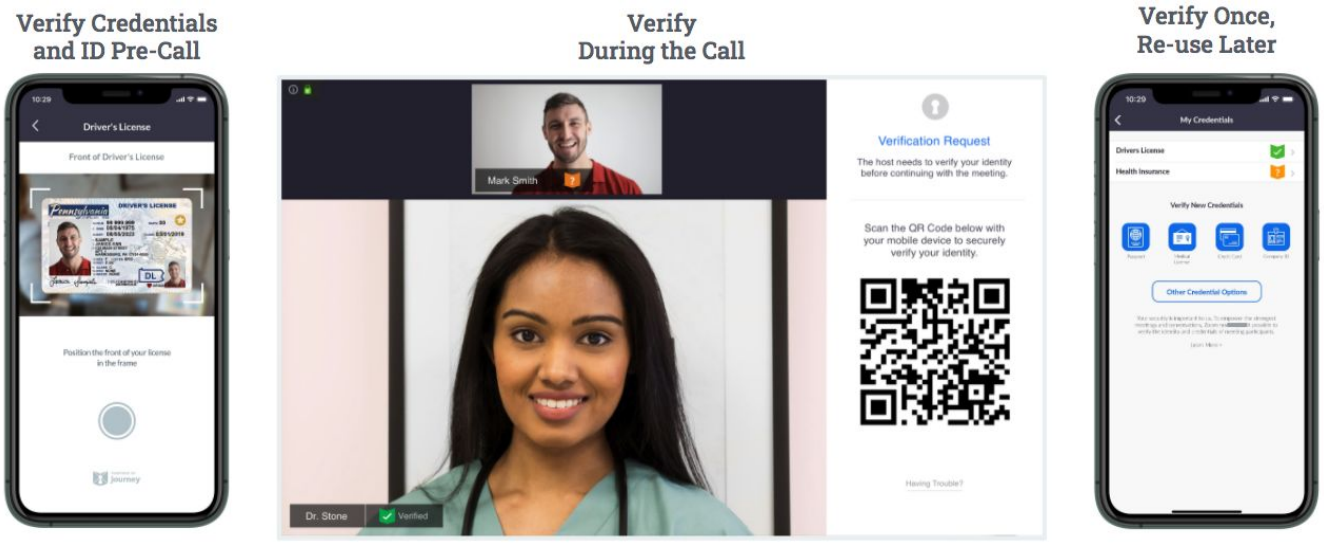



Customer + Agent Verification

## Case #2 – Secure and Trusted Healthcare Consultations

Verify the Identity & physical credentials of consultation participants, before the call or on the call. In healthcare, there are a lot of regulations around privacy and ensuring the right people can only see and interact with each other. In the diagram below that is demonstrating a telemedicine call, a caller can take a picture of their driver's license and

use it to validate their credentials, just like they would if they were attending in person.  This information can then be reused in future sessions.




## Conclusion

The internet was created without an identity layer, which has left companies and individuals vulnerable to relentless bad actors.  Many point solutions have been built over the years to address identity, but each suffered from complexity and single stores of user data that could be breached while not giving consumers some privacy controls.

Journey has solved the problem of providing great identity security while offering a great user experience in a way that also offers privacy controls.  The Journey next generation Trusted Identity Platform aims to transform the way that digital enterprises seamlessly interact.  From the initial inquiries and on-boarding to subsequent interactions, all communication is done in a highly secure, convenient, and private setting.

Journey's zero knowledge authentication obliterates the need for irritating questions about favorite pizza toppings and invokes much more secure proof of an individual's identity, in mere seconds, with user privacy controls.

## Additional Information

- www.journey.ai
- Video Demonstrations
- Contact